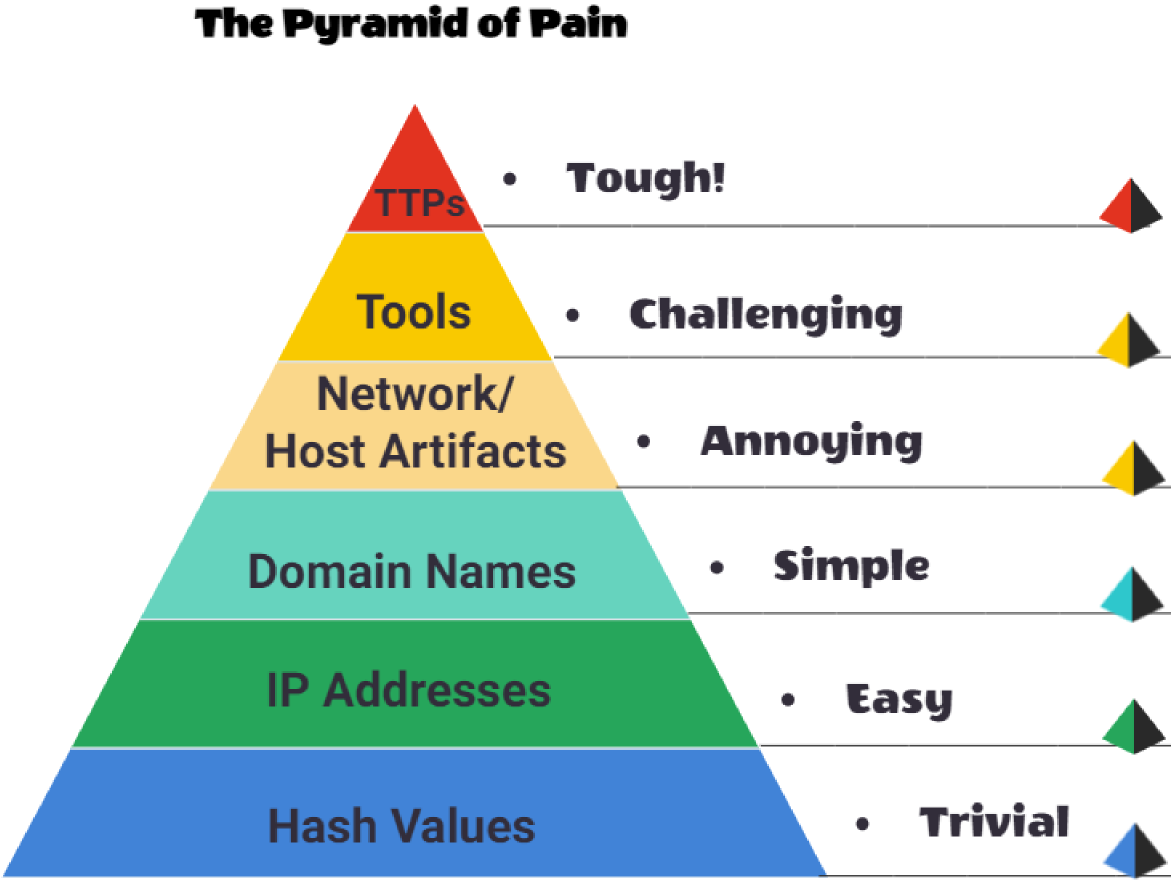
Cyber Defence Frameworks

Table of Contents

- Pyramid Of Pain
- Cyber Kill Chain
- Unified Kill Chain
- Diamond Model
- MITRE

Pyramid Of Pain

Introduction



This well-renowned concept is being applied to cybersecurity solutions like Cisco Security, SentinelOne, and SOCRadar to improve the effectiveness of CTI (Cyber Threat Intelligence), threat hunting, and incident response exercises.

Understanding the Pyramid of Pain concept as a Threat Hunter, Incident Responder, or SOC Analyst is important.

Are you ready to explore what hides inside the Pyramid of Pain?

Hash Values (Trivial)

As per Microsoft, the hash value is a numeric value of a fixed length that uniquely identifies data. A hash value is the result of a hashing algorithm. The following are some of the most common hashing algorithms:

- **MD5 (Message Digest, defined by RFC 1321**)** - was designed by Ron Rivest in 1992 and is a widely used cryptographic hash function with a 128-bit hash value. MD5 hashes are **NOT** considered **cryptographically secure**. In 2011, the IETF published RFC 6151, "Updated Security Considerations for the MD5 Message-Digest and the HMAC-MD5 Algorithms," which mentioned a number of attacks against MD5 hashes, including the hash collision.
- **SHA-1 (Secure Hash Algorithm 1, defined by RFC 3174)** - was invented by United States National Security Agency in 1995. When data is fed to SHA-1 Hashing Algorithm, SHA-1 takes an input and produces a 160-bit hash value string as a 40 digit hexadecimal number. NIST deprecated the use of SHA-1 in 2011 and banned its use for digital signatures at the end of 2013 based on it being susceptible to brute-force attacks. Instead, NIST recommends migrating from SHA-1 to stronger hash algorithms in the SHA-2 and SHA-3 families.
- **The SHA-2 (Secure Hash Algorithm 2)** - SHA-2 Hashing Algorithm was designed by The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in 2001 to replace SHA-1. SHA-2 has many variants, and arguably the most common is SHA-256. The SHA-256 algorithm returns a hash value of 256-bits as a 64 digit hexadecimal number.

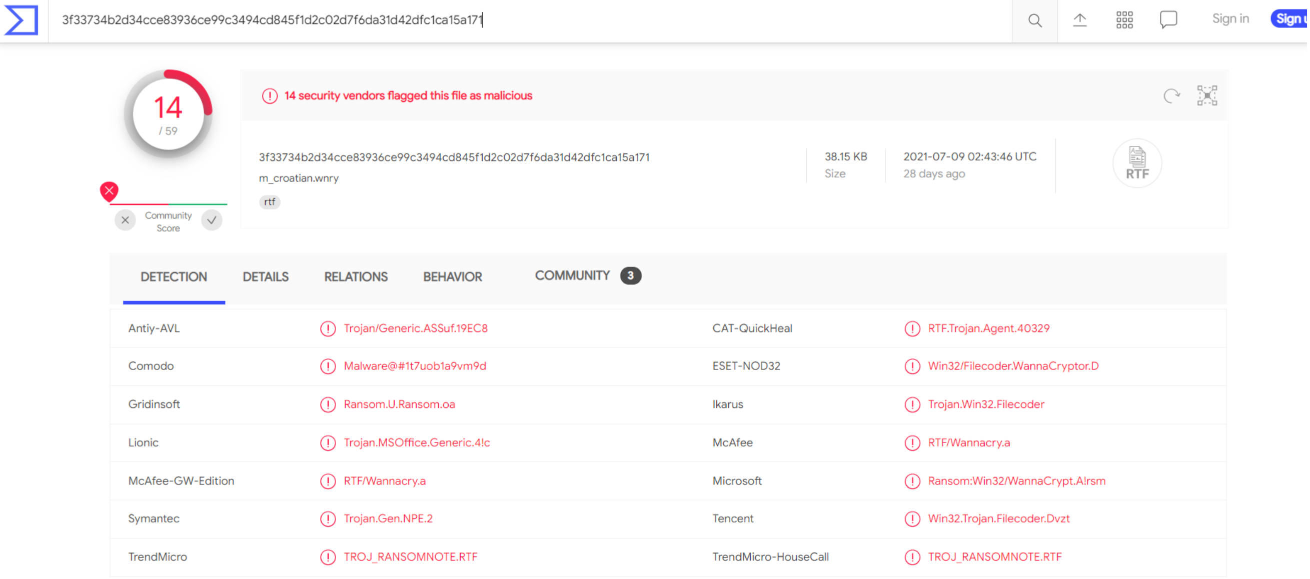
A hash is not considered to be cryptographically secure if two files have the same hash value or digest.

Security professionals usually use the hash values to gain insight into a specific malware sample, a malicious or a suspicious file, and as a way to uniquely identify and reference the malicious artifact.

You probably read the ransomware reports in the past, where security researchers would provide the hashes related to the malicious or suspicious files used at the end of the report. You can check out The DFIR Report and FireEye Threat Research Blogs if you're interested in seeing an example.

Various online tools can be used to do hash lookups like VirusTotal and Metadefender Cloud - OPSWAT.

VirusTotal:



3f33734b2d34cce83936ce99c3494cd845f1d2c02d7f6da31d42dfc1ca15a171

14 security vendors flagged this file as malicious

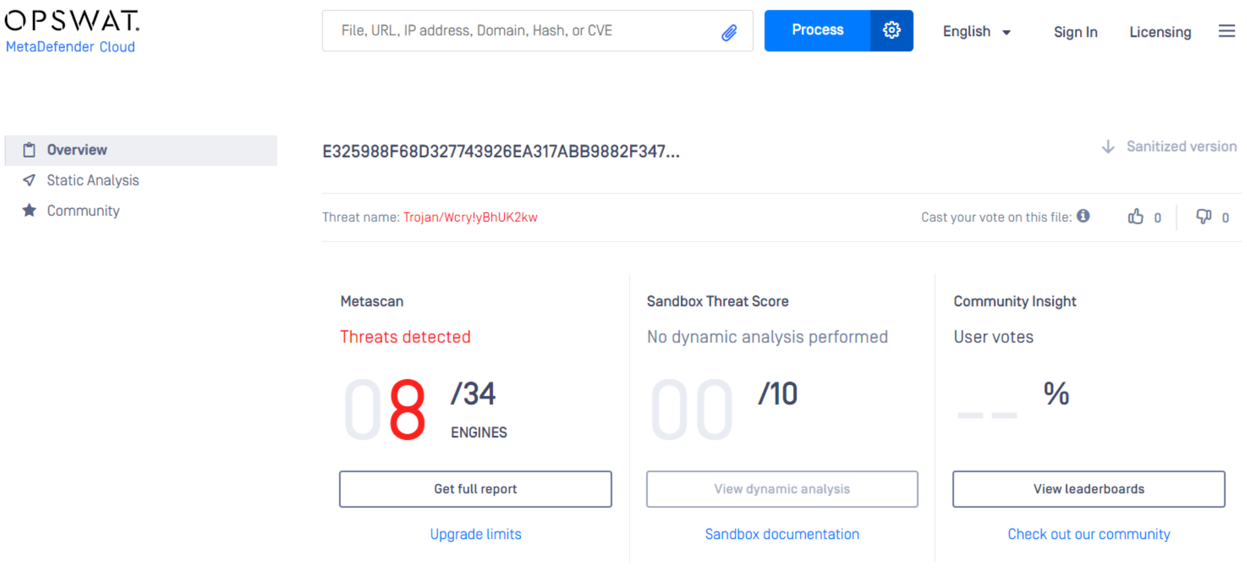
3f33734b2d34cce83936ce99c3494cd845f1d2c02d7f6da31d42dfc1ca15a171
m_croatian.wnry
rtf

38.15 KB
Size

2021-07-09 02:43:46 UTC
28 days ago

Antiy-AVL	Trojan/Generic.ASSuf.19EC8	CAT-QuickHeal	RTF.Trojan.Agent.40329
Comodo	Malware@#1t7uob1a9vm9d	ESET-NOD32	Win32/Filecoder.WannaCryptor.D
Gridinsoft	Ransom.U.Ransom.oa	Ikarus	Trojan.Win32.Filecoder
Lionic	Trojan.MSOffice.Generic.4!c	McAfee	RTF/Wannacry.a
McAfee-GW-Edition	RTF/Wannacry.a	Microsoft	Ransom:Win32/WannaCrypt.A!rsm
Symantec	Trojan.Gen.NPE.2	Tencent	Win32.Trojan.Filecoder.Dvzt
TrendMicro	TROJ_RANSOMNOTE.RTF	TrendMicro-HouseCall	TROJ_RANSOMNOTE.RTF

MetaDefender Cloud - OPSWAT:



E325988F68D327743926EA317ABB9882F347...

Threat name: Trojan/Wcry!yBhUK2kw

Cast your vote on this file: 0 0

Metascan
Threats detected
08 /34 ENGINES

Sandbox Threat Score
No dynamic analysis performed
00 /10

Community Insight
User votes
-- %

As you might have noticed, it is really easy to spot a malicious file if we have the hash in our arsenal. However, as an attacker, it's trivial to modify a file by even a single bit, which would produce a different hash value. With so many variations and instances of known malware or ransomware, threat hunting using file hashes as the IOC (Indicators of Compromise) can become a difficult task.

Let's take a look at an example of how you can change the hash value of a file by simply appending a string to the end of a file using echo: File Hash (Before Modification)

```
PS C:\Users\THM\Downloads> Get-FileHash .\OpenVPN_2.5.1_I601_amd64.msi -Algorithm MD5
Algorithm Hash                                        Path


_________ ____                                        ____

MD5       D1A008E3A606F24590A02B853E955CF7
C:\Users\THM\Downloads\OpenVPN_2.5.1_I601_amd64.msi
```

File Hash (After Modification)

```
PS C:\Users\THM\Downloads> echo "AppendTheHash" >> .\OpenVPN_2.5.1_I601_amd64.msi
PS C:\Users\THM\Downloads> Get-FileHash .\OpenVPN_2.5.1_I601_amd64.msi -Algorithm MD5
Algorithm Hash                                        Path


_________ ____                                        ____

MD5       9D52B46F5DE41B73418F8E0DACEC5E9F
C:\Users\THM\Downloads\OpenVPN_2.5.1_I601_amd64.msi
```

Provide the ransomware name for the hash '63625702e63e333f235b5025078cea1545f29b1ad42b1e46031911321779b6be' using open-source lookup tools

"conti"

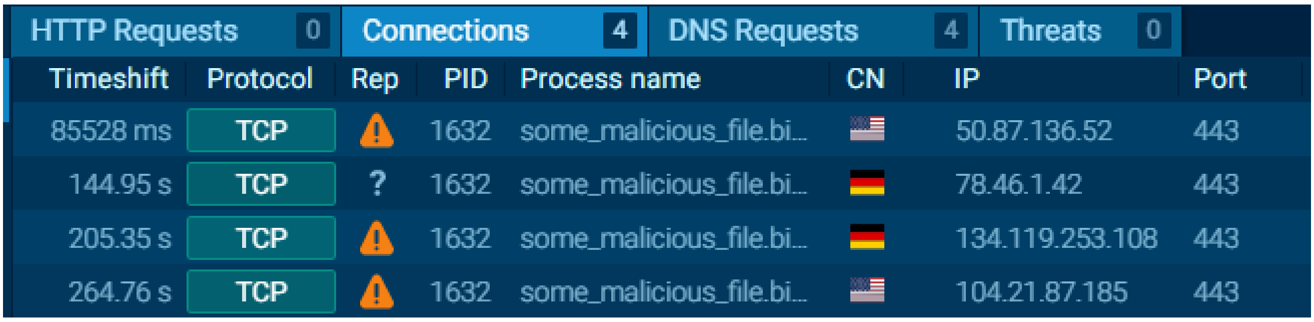
IP Address (Easy)

An IP address is used to identify any device connected to a network. These devices range from desktops, to servers and even CCTV cameras!. We rely on IP addresses to send and receive the information over the network. But we are not going to get into the structure and functionality of the IP address. As a part of the Pyramid of Pain, we'll evaluate how IP addresses are used as an indicator.

In the Pyramid of Pain, IP addresses are indicated with the color green. You might be asking why and what you can associate the green colour with?

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

Malicious IP connections (app.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

> **Note:** Do not attempt to interact with the IP addresses shown above.

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.

So, the primary concept of a Fast Flux network is having multiple IP addresses associated with a domain name, which is constantly changing. Palo Alto created a great fictional scenario to explain Fast Flux: "Fast Flux 101: How Cybercriminals Improve the Resilience of Their Infrastructure to Evade Detection and Law Enforcement Takedowns"

Use the following any.run URL to answer the questions below:

What is the ASN for the third IP address observed?

Host Europe GmbH

What is the domain name associated with the first IP address observed?

craftingalegacy.com

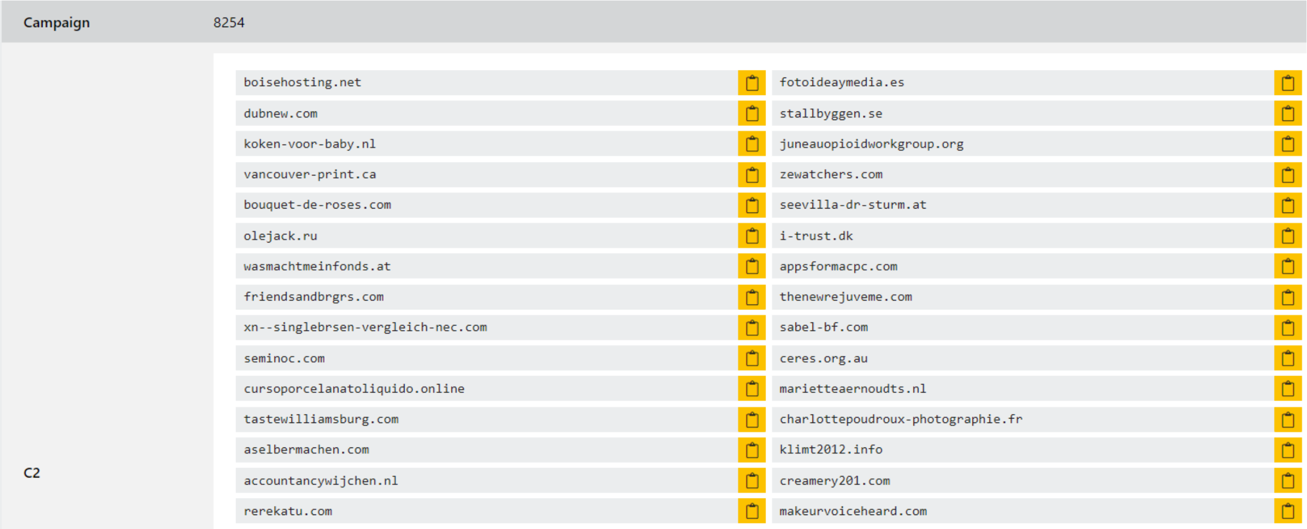
Domain Names (Simple)

Let's step up the Pyramid of Pain and move on to Domain Names. You can see the transition of colors - from green to teal.

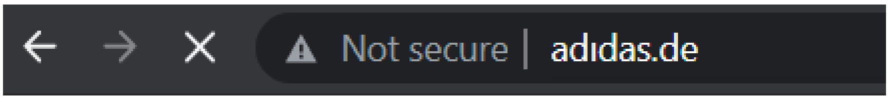
Domain Names can be thought as simply mapping an IP address to a string of text. A domain name can contain a domain and a top-level domain (evilcorp.com) or a sub-domain followed by a domain and top-level domain (tryhackme.evilcorp.com).

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.

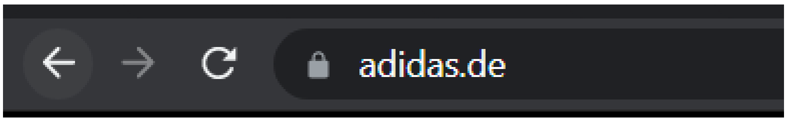
Malicious Sodinokibi C2 (Command and Control Infrastructure) **domains:**



Campaign	8254	
C2	boisehosting.net	fotoideaymedia.es
	dubnew.com	stallbyggen.se
	koken-voor-baby.nl	juneauopioidworkgroup.org
	vancouver-print.ca	zewatchers.com
	bouquet-de-roses.com	seevilla-dr-sturm.at
	olejack.ru	i-trust.dk
	wasmachtmeinfonds.at	appsformacpc.com
	friendsandbrgrs.com	thenewrejuveme.com
	xn--singlebrsen-vergleich-nec.com	sabel-bf.com
	seminoc.com	ceres.org.au
	cursoporcelanatoliquido.online	marietteaernoudts.nl
	tastewilliamsburg.com	charlottepoudroux-photographie.fr
	aselbermachen.com	klimt2012.info
	accountancywijchen.nl	creamery201.com
	rerekatu.com	makeurvoiceheard.com



Can you spot anything malicious in the above screenshot? Now, compare it to the legitimate website view below:



This is one of the examples of a Punycode attack used by the attackers to redirect users to a malicious domain that seems legitimate at first glance.

What is Punycode? As per Wandera, "Punycode is a way of converting words that cannot be written in ASCII, into a Unicode ASCII encoding."

What you saw in the URL above is `adıdas.de` which has the Punycode of `http://xn--addas-o4a.de/`

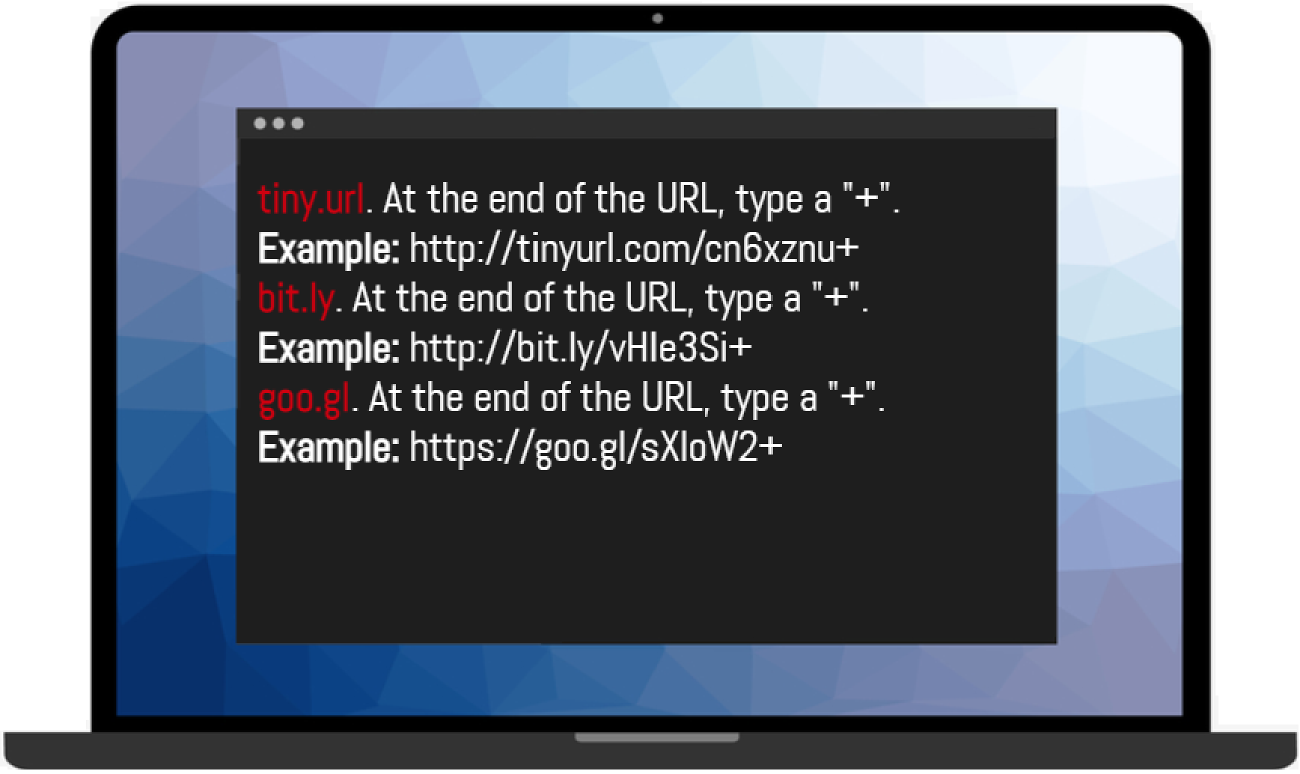
Internet Explorer, Google Chrome, Microsoft Edge, and Apple Safari are now pretty good at translating the obfuscated characters into the full Punycode domain name.

To detect the malicious domains, proxy logs or web server logs can be used.

Attackers usually hide the malicious domains under **URL Shorteners.** A URL Shortener is a tool that creates a short and unique URL that will redirect to the specific website specified during the initial step of setting up the URL Shortener link. According to Cofense, attackers use the following URL Shortening services to generate malicious links:

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

You can see the actual website the shortened link is redirecting you to by appending "+" to it (see the examples below). Type the shortened URL in the address bar of the web browser and add the above characters to see the redirect URL.



tiny.url. At the end of the URL, type a "+".
Example: http://tinyurl.com/cn6xznu+
bit.ly. At the end of the URL, type a "+".
Example: http://bit.ly/vHIe3Si+
goo.gl. At the end of the URL, type a "+".
Example: https://goo.gl/sXIoW2+

Go to this report on app.any.run and provide the first malicious URL request you are seeing, you will be using this report to answer the remaining questions of this task.

craftingalegacy.com

What term refers to an address used to access websites?

Domain Name

What type of attack uses Unicode characters in the domain name to imitate the a known domain?

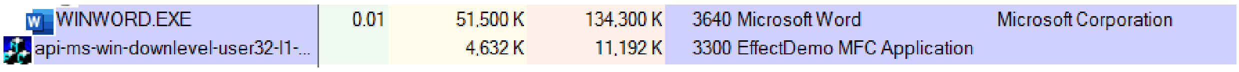
Punycode attack

Host Artifacts (Annoying)

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.

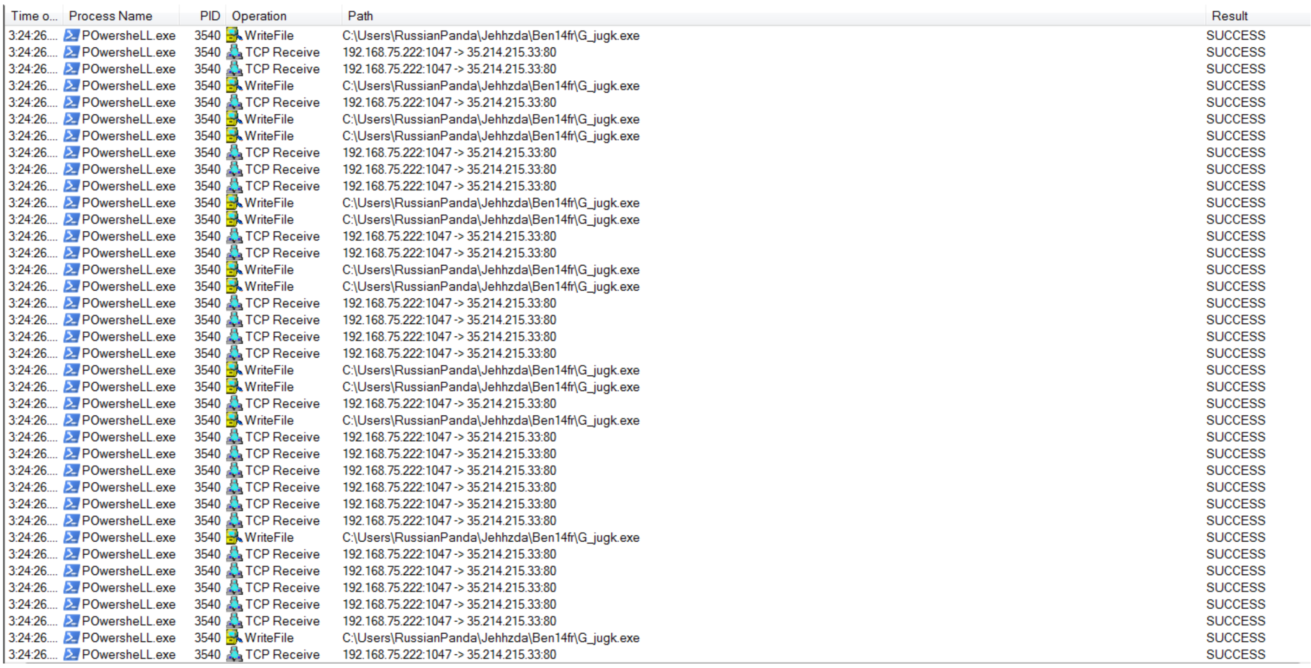
Host artifacts are the traces or observables that attackers leave on the system, such as registry values, suspicious process execution, attack patterns or IOCs (Indicators of Compromise), files dropped by malicious applications, or anything exclusive to the current threat.

Suspicious process execution from Word:



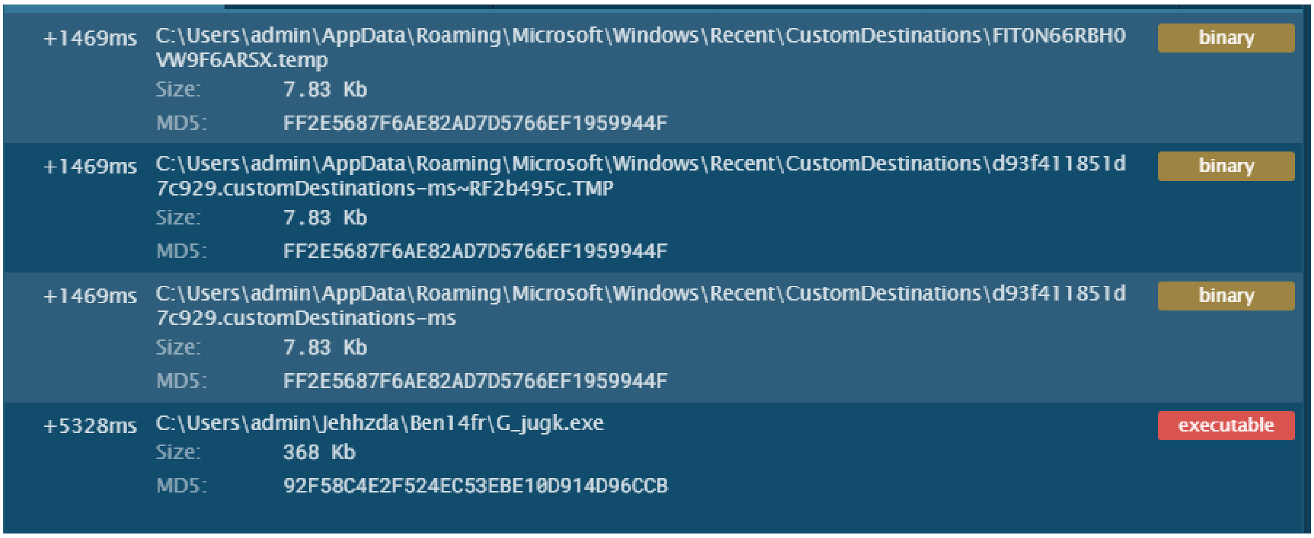
WINWORD.EXE	0.01	51,500 K	134,300 K	3640 Microsoft Word	Microsoft Corporation
api-ms-win-downlevel-user32-l1-...		4,632 K	11,192 K	3300 EffectDemo MFC Application	

Suspicious events followed by opening a malicious application:



Time o...	Process Name	PID	Operation	Path	Result
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS
3:24:26....	POwersheLL.exe	3540	WriteFile	C:\Users\RussianPanda\Jehhzda\Ben14fr\G_jugk.exe	SUCCESS
3:24:26....	POwersheLL.exe	3540	TCP Receive	192.168.75.222:1047 -> 35.214.215.33:80	SUCCESS

The files modified/dropped by the malicious actor:



+1469ms	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FITON66RBH0VW9F6ARSX.temp Size: 7.83 Kb MD5: FF2E5687F6AE82AD7D5766EF1959944F	binary
+1469ms	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms~RF2b495c.TMP Size: 7.83 Kb MD5: FF2E5687F6AE82AD7D5766EF1959944F	binary
+1469ms	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms Size: 7.83 Kb MD5: FF2E5687F6AE82AD7D5766EF1959944F	binary
+5328ms	C:\Users\admin\Jehhzda\Ben14fr\G_jugk.exe Size: 368 Kb MD5: 92F58C4E2F524EC53EBE10D914D96CCB	executable

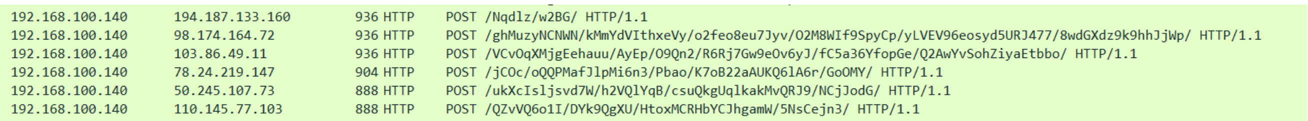
Network Artifacts (Annoying)

Network Artifacts also belong to the yellow zone in the Pyramid of Pain. This means if you can detect and respond to the threat, the attacker would need more time to go back and change his tactics or modify the tools, which gives you more time to respond and detect the upcoming threats or remediate the existing ones.

A network artifact can be a user-agent string, C2 information, or URI patterns followed by the HTTP POST requests. An attacker might use a User-Agent string that hasn't been observed in your environment before or seems out of the ordinary. The User-Agent is defined by RFC2616 as the request-header field that contains the information about the user agent originating the request.

Network artifacts can be detected in Wireshark PCAPs (file that contains the packet data of a network) by using a network protocol analyser such as TShark or exploring IDS (Intrusion Detection System) logging from a source such as Snort.

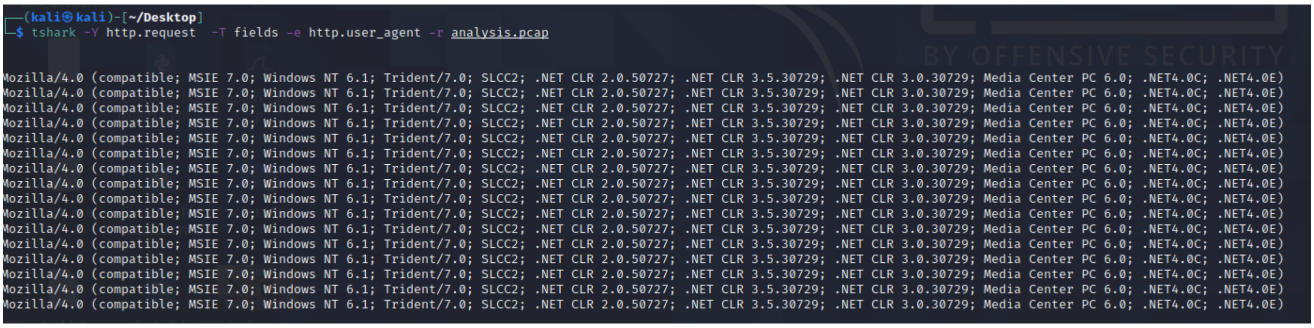
HTTP POST requests containing suspicious strings:



```
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
```

Let's use TShark to filter out the User-Agent strings by using the following command:

```
tshark --Y http.request -T fields -e http.host -e http.user_agent -r analysis_file.pcap
```



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


Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
Mozilla/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)
```

These are the most common User-Agent strings found for the Emotet Downloader Trojan

If you can detect the custom User-Agent strings that the attacker is using, you might be able to block them, creating more obstacles and making their attempt to compromise the network more annoying.

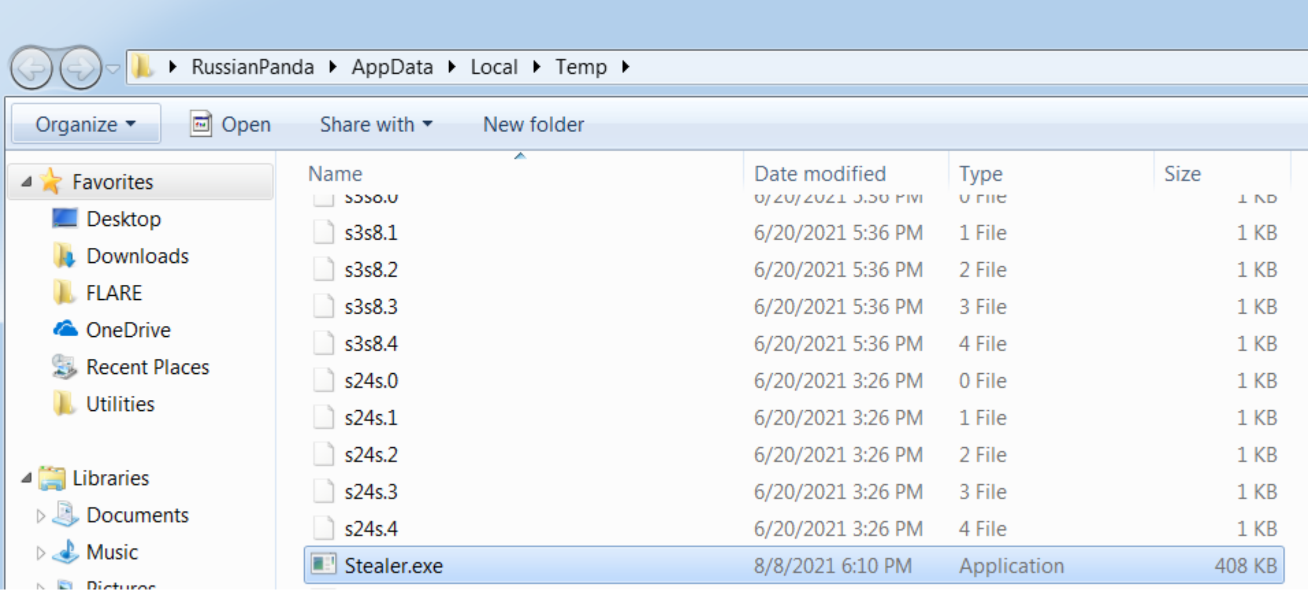
Tools (Challenging)

Congratulations! We have made it to the challenging part for the adversaries!

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 are capable of doing so), find the tool that has the same potential, or even gets some training to learn how to be proficient in a certain tool.

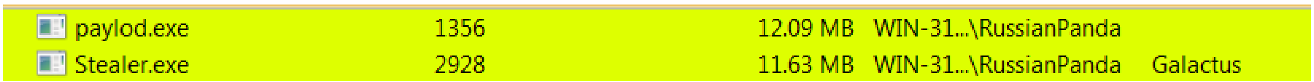
Attackers would use the utilities to create malicious macro documents (maldocs) for spearphishing attempts, a backdoor that can be used to establish C2 (Command and Control Infrastructure), any custom .EXE, and .DLL files, payloads, or password crackers.

A Trojan dropped the suspicious "Stealer.exe" in the Temp folder:



Name	Date modified	Type	Size
s3s8.0	6/20/2021 5:36 PM	0 File	1 KB
s3s8.1	6/20/2021 5:36 PM	1 File	1 KB
s3s8.2	6/20/2021 5:36 PM	2 File	1 KB
s3s8.3	6/20/2021 5:36 PM	3 File	1 KB
s3s8.4	6/20/2021 5:36 PM	4 File	1 KB
s24s.0	6/20/2021 3:26 PM	0 File	1 KB
s24s.1	6/20/2021 3:26 PM	1 File	1 KB
s24s.2	6/20/2021 3:26 PM	2 File	1 KB
s24s.3	6/20/2021 3:26 PM	3 File	1 KB
s24s.4	6/20/2021 3:26 PM	4 File	1 KB
Stealer.exe	8/8/2021 6:10 PM	Application	408 KB

The execution of the suspicious binary:



paylod.exe	1356	12.09 MB	WIN-31...\RussianPanda	
Stealer.exe	2928	11.63 MB	WIN-31...\RussianPanda	Galactus

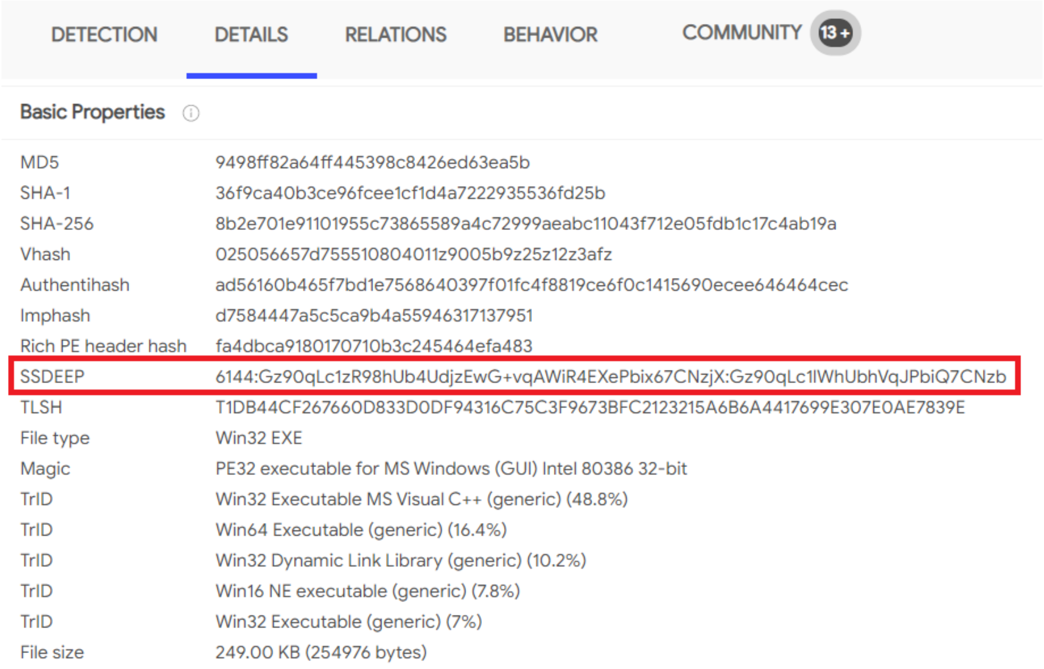
Antivirus signatures, detection rules, and YARA rules can be great weapons for you to use against attackers at this stage.

MalwareBazaar and Malshare are good resources to provide you with access to the samples, malicious feeds, and YARA results - these all can be very helpful when it comes to threat hunting and incident response.

For detection rules, SOC Prime Threat Detection Marketplace is a great platform, where security professionals share their detection rules for different kinds of threats including the latest CVE's that are being exploited in the wild by adversaries.

Fuzzy hashing is also a strong weapon against the attacker's tools. Fuzzy hashing helps you to perform similarity analysis - match two files with minor differences based on the fuzzy hash values. One of the examples of fuzzy hashing is the usage of SSDeep; on the SSDeep official website, you can also find the complete explanation for fuzzy hashing.

Example of SSDeep from VirusTotal:



Basic Properties

MD5	9498ff82a64ff445398c8426ed63ea5b
SHA-1	36f9ca40b3ce96fcee1cf1d4a7222935536fd25b
SHA-256	8b2e701e91101955c73865589a4c72999aeabc11043f712e05fdb1c17c4ab19a
Vhash	025056657d755510804011z9005b9z25z12z3afz
Authentihash	ad56160b465f7bd1e7568640397f01fc4f8819ce6f0c1415690ecee646464cec
Imphash	d7584447a5c5ca9b4a55946317137951
Rich PE header hash	fa4dbca9180170710b3c245464efa483
SSDEEP	6144:Gz90qLc1zR98hUb4UdjzEwG+vqAWiR4EXePbix67CNzjX:Gz90qLc1lWhUbhVqJPbiQ7CNzb
TLSH	T1DB44CF267660D833D0DF94316C75C3F9673BFC2123215A6B6A4417699E307E0AE7839E
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 Executable MS Visual C++ (generic) (48.8%)
TrID	Win64 Executable (generic) (16.4%)
TrID	Win32 Dynamic Link Library (generic) (10.2%)
TrID	Win16 NE executable (generic) (7.8%)
TrID	Win32 Executable (generic) (7%)
File size	249.00 KB (254976 bytes)

TTPs (Tough)

TTPs stands for Tactics, Techniques & Procedures. This includes the whole MITRE ATT&CK Matrix, which means all the steps taken by an adversary to achieve his goal, starting from phishing attempts to persistence and data exfiltration.

If you can detect and respond to the TTPs quickly, you leave the adversaries almost no chance to fight back. 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:

1. Go back, do more research and training, reconfigure their custom tools
2. Give up and find another target

Option 2 definitely sounds less time and resource-consuming.

Navigate to ATT&CK Matrix webpage. How many techniques fall under the Exfiltration category?

Chimera is a China-based hacking group that has been active since 2018. What is the name of the commercial, remote access tool they use for C2 beacons and data exfiltration?

Cobalt Strike

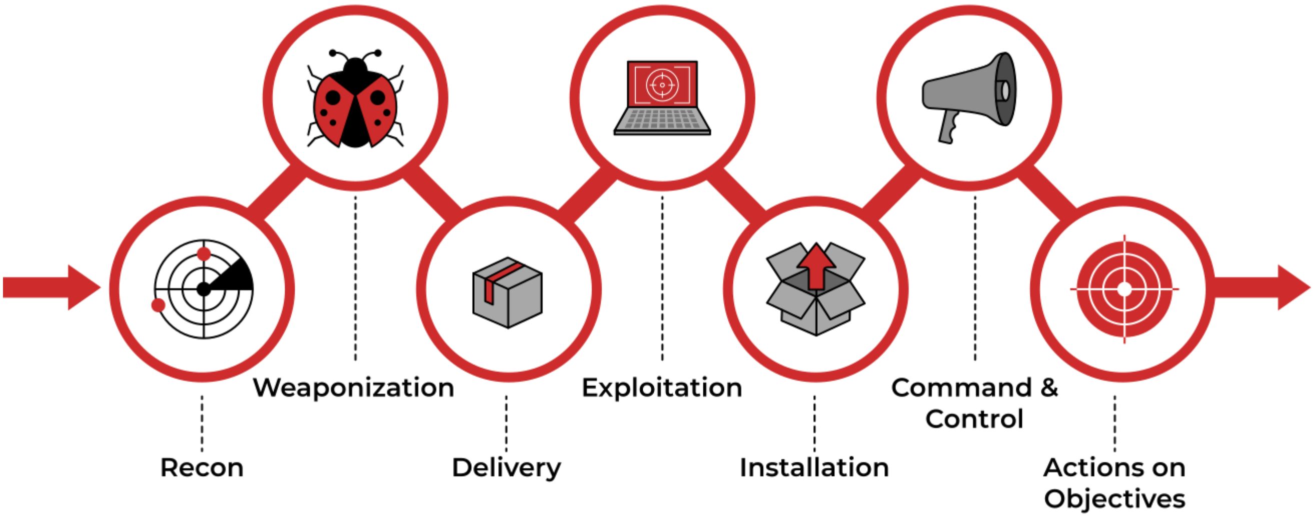
Conclusion

Now you have learned the concept of the Pyramid of Pain. Maybe it is time to apply this in practice. Please, navigate to the Static Site to perform the exercise.

You can pick any APT (Advanced Persistent Threat Groups) as another exercise. A good place to look at would be FireEye Advanced Persistent Threat Groups. When you have determined the APT Group you want to research - find their indicators and ask yourself: " What can I do or what detection rules and approach can I create to detect the adversary's activity?", and "Where does this activity or detection fall on the Pyramid of Pain?”

Cyber Kill Chain

Introduction



The term **kill chain** is a military concept related to the structure of an attack. It consists of target identification, decision and order to attack the target, and finally the target destruction.

Thanks to Lockheed Martin, a global security and aerospace company, that established the Cyber Kill Chain® framework for the cybersecurity industry in 2011 based on the military concept. The 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. We will go through the attack phases and help you better understand adversaries and their techniques used in the attack to defend yourself.

So, why is it important to understand how Cyber Kill Chain works?

The Cyber Kill Chain will help you understand and protect against ransomware attacks, security breaches as well as Advanced Persistent Threats (APTs). You can use the Cyber Kill Chain to assess your network and system security by identifying missing security controls and closing certain security gaps based on your company's infrastructure.

By understanding the Kill Chain as a SOC Analyst, Security Researcher, Threat Hunter, or Incident Responder, you will be able to recognize the intrusion attempts and understand the intruder's goals and objectives.

We will be exploring the following attack phases in this room:

- Reconnaissance
- Weaponization
- Delivery
- Exploitation
- Installation
- Command & Control
- Actions on Objectives

Learning Objectives: In this room, you will learn about each phase of the Cyber Kill Chain Framework, the advantages and disadvantages of the traditional Cyber Kill Chain.

Outcome: As a result, you will be ready to recognise different phases or stages of the attack carried out by an adversary and be able to break the "kill chain."

Reconnaissance

To learn what reconnaissance is from the attacker's perspective, first, let's define the term **reconnaissance.**

Reconnaissance is discovering and collecting information on the system and the victim. The reconnaissance phase is the planning phase for the adversaries.

OSINT (Open-Source Intelligence) also falls under reconnaissance. OSINT is the first step an attacker needs to complete to carry out the further phases of an attack. The attacker needs to study the victim by collecting every available piece of information on the company and its employees, such as the company's size, email addresses, phone numbers from publicly available resources to determine the best target for the attack.

You can also find out more about OSINT from this Varonis article, "What is OSINT?"

Let's look at it from the attacker's perspective, who initially doesn't know what company he wants to attack.

Here is the scenario: A malicious attacker who names himself "Megatron" decides to conduct a very sophisticated attack that he has been planning out for years; he has been studying and researching different tools and techniques that could help him get to the last phase of the Cyber Kill Chain. But first, he needs to start from the Reconnaissance phase.

In order to operate in this phase, the attacker would need to conduct OSINT. Let's have a look at Email harvesting.

Email harvesting is the process of obtaining email addresses from public, paid, or free services. An attacker can use email-address harvesting for a **phishing attack** (a type of social-engineering attack used to steal sensitive data, including login credentials and credit card numbers). The attacker will have a big arsenal of tools available for reconnaissance purposes. Here are some of them:

theHarvester - other than gathering emails, this tool is also capable of gathering names, subdomains, IPs, and URLs using multiple public data sources

Hunter.io - this is an email hunting tool that will let you obtain contact information associated with the domain

OSINT Framework - OSINT Framework provides the collection of OSINT tools based on various categories

An attacker would also use social media websites such as LinkedIn, Facebook, Twitter, and Instagram to collect information on a specific victim he would want to attack or the company. The information found on social media can be beneficial for an attacker to conduct a phishing attack.

Weaponization

After a successful reconnaissance stage, "Megatron" would work on crafting a "weapon of destruction". He would prefer not to interact with the victim directly and, instead, he will create a "weaponizer" that, according to Lockheed Martin, combines **malware** and **exploit** into a deliverable **payload**. Most attackers usually use automated tools to generate the malware or refer to the DarkWeb to purchase the malware. More sophisticated actors or nation-sponsored APT (Advanced Persistent Threat Groups) would write their custom malware to make the malware sample unique and evade detection on the target.

Let's first define some terminology before we analyze the Weaponization phase.

Malware is a program or software that is designed to damage, disrupt, or gain unauthorized access to a computer.

An **exploit** is a program or a code that takes advantage of the vulnerability or flaw in the application or system.

A **payload** is a malicious code that the attacker runs on the system.

Continuing with our adversary, "Megatron" chooses...

"Megatron" chooses to buy an already written payload from someone else in the DarkWeb, so that he can spend more time on the other phases.

In the Weaponization phase, the attacker would:

- Create an infected Microsoft Office document containing a malicious macro or VBA (Visual Basic for Applications) scripts. If you want to learn about macro and VBA, please refer to the article "Intro to Macros and VBA For Script Kiddies" by TrustedSec.
- 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.
- 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.
- An attacker would select a **backdoor** implant (the way to access the computer system, which includes bypassing the security mechanisms).

Delivery

The Delivery phase is when "Megatron" decides to choose the method for transmitting the payload or the malware. He has plenty of options to choose from:

- Phishing email: after conducting the reconnaissance and determining the targets for the attack, the malicious actor would craft a malicious email that would target either a specific person (spearphishing attack) or multiple people in the company. The email would contain a payload or malware. For example, "Megatron" would learn that Nancy from the Sales department at company A would constantly like the posts on LinkedIn from Scott, a Service Delivery Manager at company B. He would give it a second guess that they both communicate with each other over work emails. "Megatron" would craft an email using Scott's First Name and Last Name, making the domain look similar to the company Scott is working at. An attacker would then send a fake "Invoice" email to Nancy, which contains the payload.

- Distributing infected USB drives in public places like coffee shops, parking lots, or on the street. An attacker might decide to conduct a sophisticated USB Drop Attack by printing the company's logo on the USB drives and mailing them to the company while pretending to be a customer sending the USB devices as a gift. You can read about one of these similar attacks at CSO Online "Cybercriminal group mails malicious USB dongles to targeted companies."
- Watering hole attack. A watering hole attack is a targeted attack designed to aim at a specific group of people by compromising the website they are usually visiting and then redirecting them to the malicious website of an attacker's choice. The attacker would look for a known vulnerability for the website and try to exploit it. The attacker would encourage the victims to visit the website by sending "harmless" emails pointing out the malicious URL to make the attack work more efficiently. After visiting the website, the victim would unintentionally download malware or a malicious application to their computer. This type of attack is called a drive-by download. An example can be a malicious pop-up asking to download a fake Browser extension.

Exploitation

To gain access to the system, an attacker needs to exploit the vulnerability. In this phase, "Megatron" got a little bit creative - he created two phishing emails, one that contains a phishing link to a fake Office 365 login page and another one containing a macro attachment that would execute ransomware when the victim opens it. "Megatron" successfully delivered his exploits and got two victims to click on the malicious link and open the malicious file.

After gaining access to the system, the malicious actor could exploit software, system, or server-based vulnerabilities to escalate the privileges or move laterally through the network. According to CrowdStrike, **lateral movement** refers to the techniques that a malicious actor uses after gaining initial access to the victim's machine to move deeper into a network to obtain sensitive data.

If you want to learn more about server-based or web-based vulnerabilities, please refer to the TryHackMe room OWASP Top 10.

The attacker might also apply a "Zero-day Exploit" in this stage. According to FireEye, *"the 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."*

These are examples of how an attacker carries out exploitation:

- The victim triggers the exploit by opening the email attachment or clicking on a malicious link.
- Using a zero-day exploit.
- Exploit software, hardware, or even human vulnerabilities.
- An attacker triggers the exploit for server-based vulnerabilities.

Installation

As you have learned from the Weaponization phase, the backdoor lets an attacker bypass security measures and hide the access. A backdoor is also known as an access point.

Once the attacker gets access to the system, he would want to reaccess the system if he loses the connection to it or if he got detected and got the initial access removed, or if the system is later patched. He will no longer have access to it. That is when the attacker needs to install a **persistent backdoor.** A persistent backdoor will let the attacker access the system he compromised in the past. You can check out the Persistence Room on TryHackMe to learn how an attacker can achieve persistence.

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 the 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 the 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.

Command & Control

After getting persistence and executing the malware on the victim's machine, "Megatron" opens up the C2 (Command and Control) channel through the malware 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. The infected host will consistently communicate with the C2 server; that is also where the beaconing term came from.

The compromised endpoint would communicate with an external server set up by an attacker to establish a command & control channel. After establishing the connection, the attacker has full control of the victim's machine. Until recently, IRC (Internet Relay Chat) was the traditional C2 channel used by attackers. This is no longer the case, as modern security solutions can easily detect malicious IRC traffic.

The most common C2 channels used by adversaries nowadays:

- The protocols HTTP on port 80 and HTTPS on port 443 - this type of beaconing blends the malicious traffic with the legitimate traffic and can help the attacker evade firewalls.
- DNS (Domain Name Server). The infected machine makes constant DNS requests to the DNS server that belongs to an attacker, this type of C2 communication is also known as DNS Tunneling.

Important to note that an adversary or another compromised host can be the owner of the C2 infrastructure.

Actions on Objectives (Exfiltration)

After going through six phases of the attack, "Megatron" can finally achieve his goals, which means taking action on the original objectives. With hands-on keyboard access, the attacker can achieve the following:

- 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.

Conclusion

Cyber Kill Chain can be a great tool to improve network defence. Is it perfect and can it be the only tool to rely on? No.

The traditional Cyber Kill Chain or Lockheed Martin Cyber Kill Chain was last modified in 2011, which, if you remember, is the date of its establishment. The absence of updates and modifications creates security gaps.

The traditional Cyber Kill Chain was designed to secure the network perimeter and protect against malware threats. But the cybersecurity threats have developed drastically nowadays, and adversaries are combining multiple TTP (tactics, techniques, and procedures) to achieve their goal. Adversaries are capable of defeating threat intelligence by modifying the file hashes and IP addresses. Security solutions companies are developing technologies like AI (Artificial Intelligence) and different algorithms to detect even slight and suspicious changes.

Since the main focus of the framework is on malware delivery and network security, the traditional Cyber Kill Chain will not be able to identify **Insider Threats**. According to CISA, *"The Insider Threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization."*

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

Understanding the behaviours, objectives and methodologies of a cyber threat is a vital step to establishing a strong cybersecurity defence (known as a cybersecurity posture).

In this room, you will be introduced to the UKC (Unified Kill Chain) framework that is used to help understand how cyber attacks occur.

Learning Objectives:

- Understanding why frameworks such as the UKC are important and helpful in establishing a good cybersecurity posture
- Using the UKC to understand an attacker's motivation, methodologies and tactics
- Understanding the various phases of the UKC

- Discover that the UKC is a framework that is used to complement other frameworks such as MITRE.

What is a "Kill Chain"

Originating from the military, a “Kill Chain” is a term used to explain the various stages of an attack. In the realm of cybersecurity, a “Kill Chain” is used to describe the methodology/path attackers such as hackers or APTs use to approach and intrude a target.

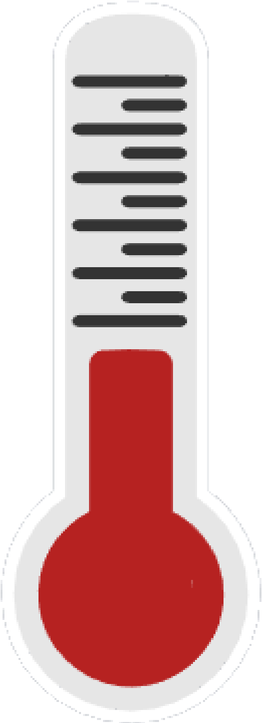
For example, an attacker scanning, exploiting a web vulnerability, and escalating privileges will be a “Kill Chain”. We will come to explain these stages in much further detail later in this room.

The objective is to understand an attacker's “Kill Chain” so that defensive measures can be put in place to either pre-emptively protect a system or disrupt an attacker's attempt.

What is "Threat Modelling"

Threat modelling, in a cybersecurity context, is a series of steps to ultimately improve the security of a system. Threat modelling is about identifying risk and essentially boils down to:

1. Identifying what systems and applications need to be secured and what function they serve in the environment. For example, is the system critical to normal operations, and is a system holding sensitive information like payment info or addresses?
2. Assessing what vulnerabilities and weaknesses these systems and applications may have and how they could be potentially exploited
3. Creating a plan of action to secure these systems and applications from the vulnerabilities highlighted
4. Putting in policies to prevent these vulnerabilities from occurring again where possible (for example, implementing a software development life cycle (SDLC) for an application or training employees on phishing awareness).



Threat modelling is an important procedure in reducing the risk within a system or application, as it creates a high-level overview of an organisation's IT assets (*an asset in IT is a piece of software or hardware*) and the procedures to resolve vulnerabilities.

The UKC can encourage threat modelling as the UKC framework helps identify potential attack surfaces and how these systems may be exploited.

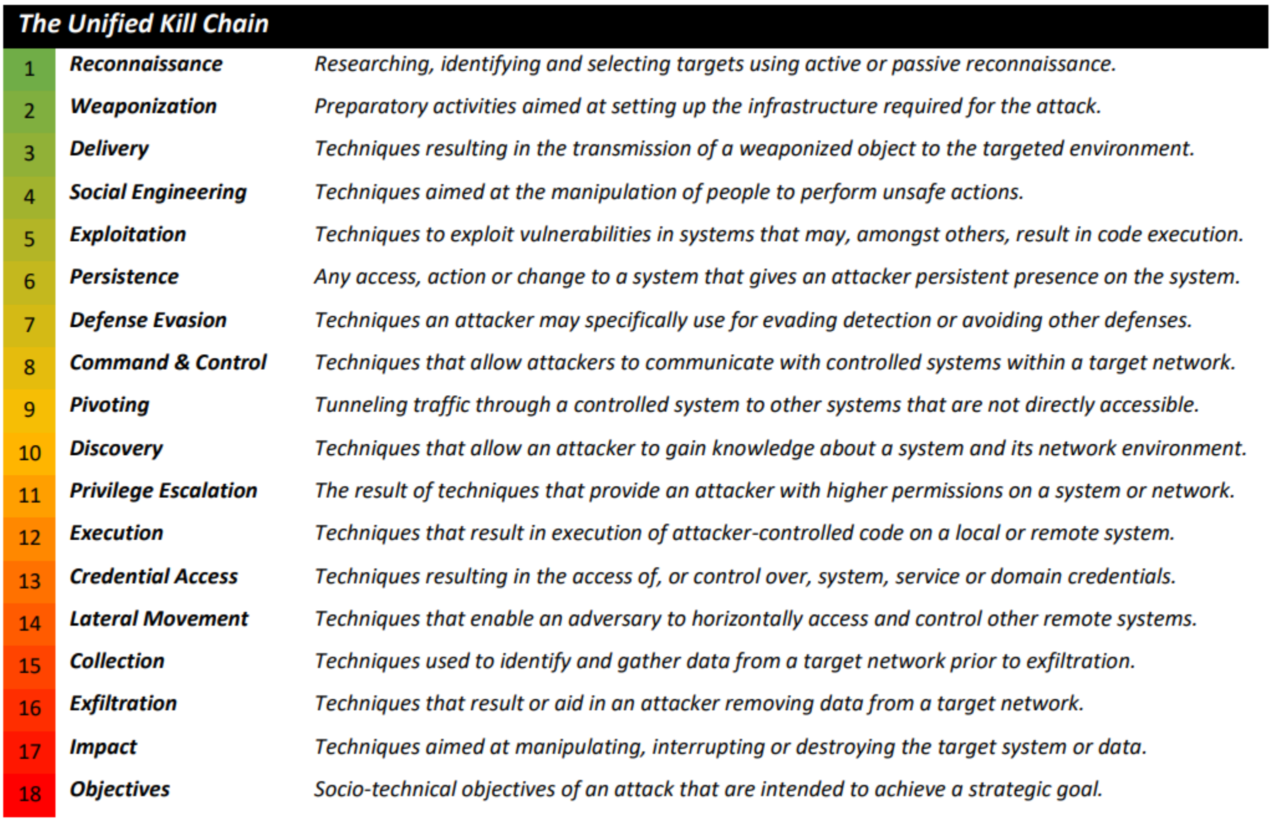
STRIDE, DREAD and CVSS (to name a few) are all frameworks specifically used in threat modelling. If you are interested to learn more, check out the “Principles of Security” room on TryHackMe.

Introducing the Unified Kill Chain

To continue from the previous task, the Unified Kill Chain published in 2017, aims to complement (**not compete**) with other cybersecurity kill chain frameworks such as Lockheed Martin’s and MITRE’s ATT&CK.

The UKC states that there are 18 phases to an attack: Everything from reconnaissance to data exfiltration and understanding an attacker's motive. These phases have been grouped together in this room into a few areas of focus for brevity, which will be detailed in the remaining tasks.

Some large benefits of the UKC over traditional cybersecurity kill chain frameworks include the fact that it is modern and extremely detailed (**reminder**: it has 18 phases officially, whereas other frameworks may have a small handful)



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 Unified Kill Chain (UKC) Framework	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 amount 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.

Phase: In (Initial Foothol)

The main focus of this series of phases is for an attacker to gain access to a system or networked environment.

An attacker will employ numerous tactics to investigate the system for potential vulnerabilities that can be exploited to gain a foothold in the system. For example, a common tactic is the use of reconnaissance against a system to discover potential attack vectors (such as applications and services).

<img src="https://tryhackme-images.s3.amazonaws.com/user-uploads/5de96d9ca744773ea7ef8c00/room-content/7b2d991f38d302d49b0d1898448e2be8.png" alt="a picture of the in section of the UKC framework style="zoom:80%;" >

Attackers employ all kinds of tactics in this stage to initiate a foothold, including:

1. Exploiting a vulnerable application or service
2. Phishing attacks
3. Supply-chain attacks
4. Social Engineering

<p style=" />

We will explore the different phases of this section of the UKC in the headings below:

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).

Information gathered from this phase can include:

- Discovering what systems and services are running on the target, this is beneficial information in the weaponisation 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.

This phase is valuable when analysing an attack as it helps form a response and better yet - gives the defensive team information on how they can improve their defence systems in the future.

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.

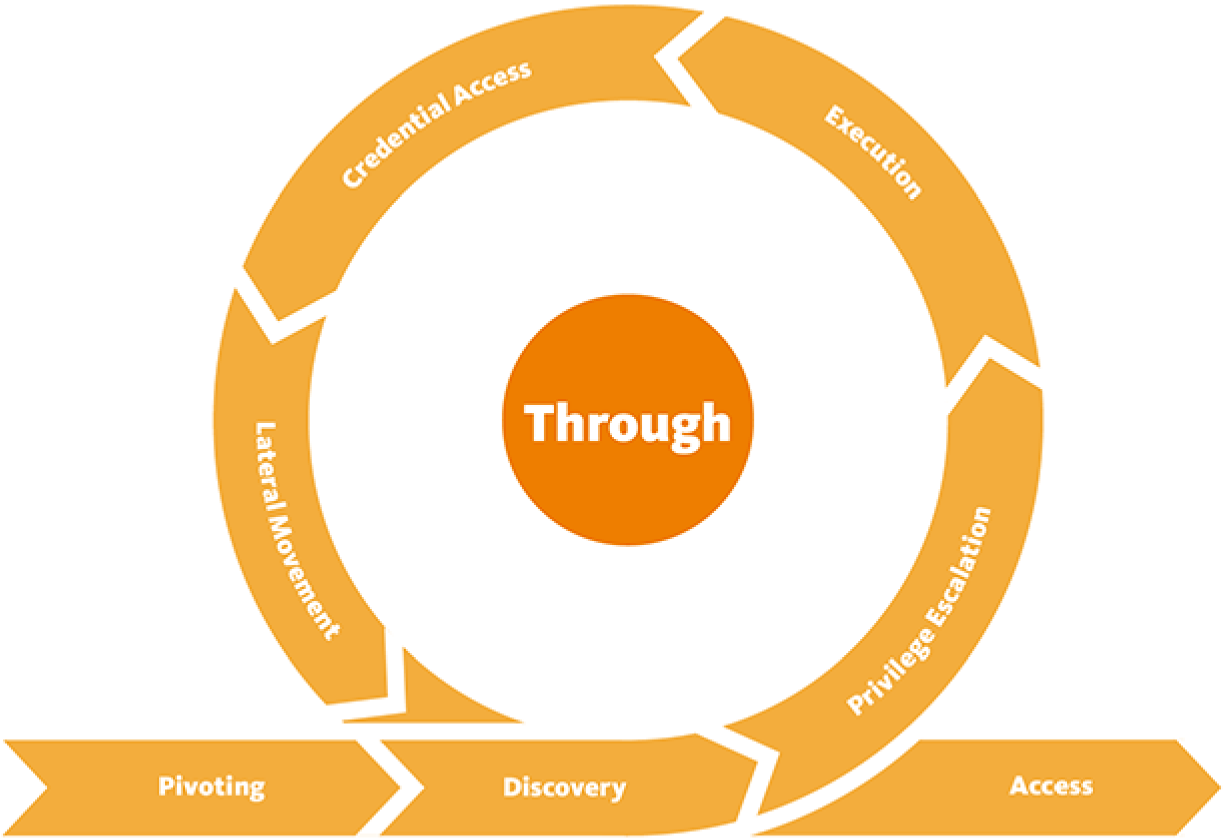
Pivoting (MITRE Tactic TA0008)

"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 publically accessible to attack other systems that are within the same network (but are not accessible via the internet).

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.



Lateral Movement (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 infrastructureOnce 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)

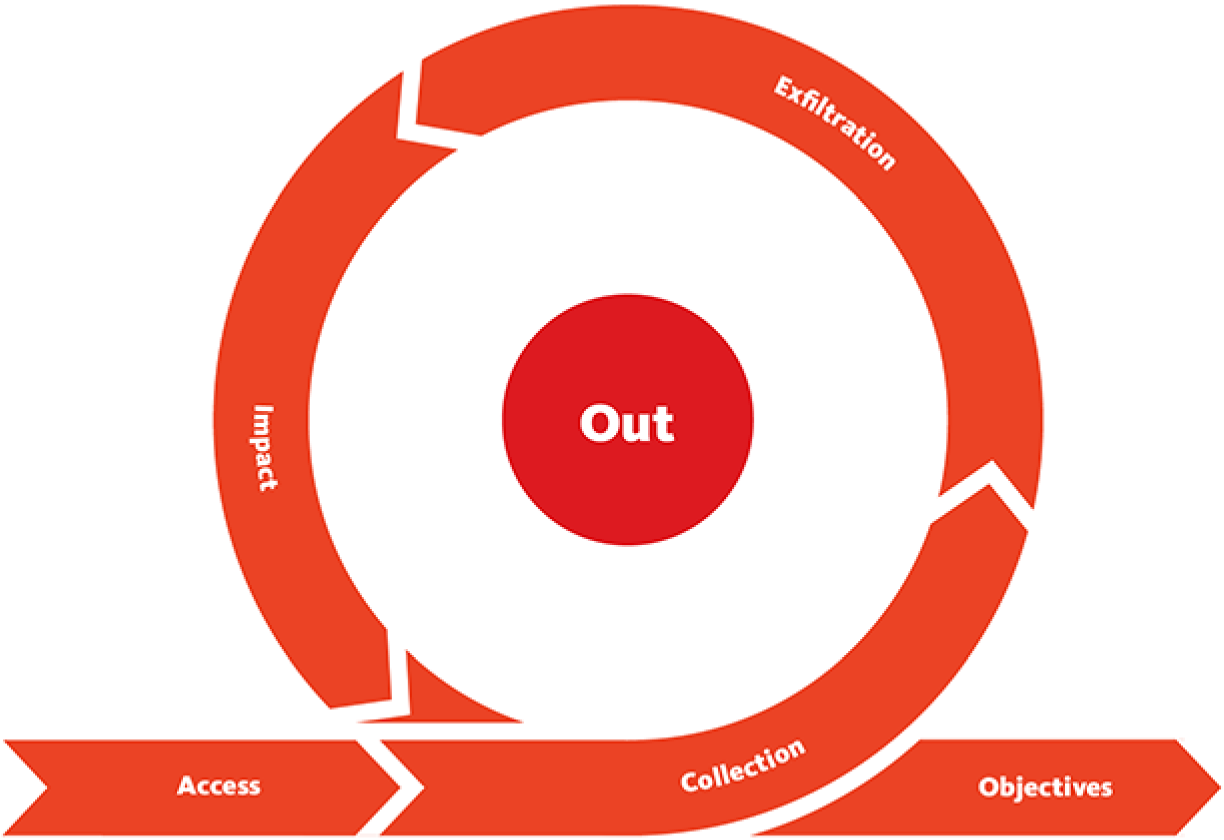
Working hand in hand with the Privilege Escalation stage, the adversary would attempt to steal account names and passwords through various methods, including keylogging and credential dumping. This makes them harder to detect during their attack as they would be using legitimate credentials.

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.

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.



The tactics to be deployed by an attacker would include:

Collection MITRE Tactic (TA0009)

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

Introduction

What is The Diamond Model?

The Diamond Model of Intrusion Analysis was developed by cybersecurity professionals - Sergio Caltagirone, Andrew Pendergast, and Christopher Betz in 2013.

As described by its creators, the Diamond Model is composed of four core features: adversary, infrastructure, capability, and victim, and establishes the fundamental atomic element of any intrusion activity. You might have also noticed two additional components or axes of the Diamond Model - Social, Political and Technology; we will go into a little bit more detail about them later in this room. Why is it called a "Diamond Model"? The four core features are edge-connected, representing their underlying relationships and arranged in the shape of a diamond.

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 defence, automating correlation across events, classifying events with confidence into adversary campaigns, and forecasting adversary operations while planning and gaming mitigation strategies.

The Diamond Model can help you identify the elements of an intrusion. At the end of this room, you will create a Diamond Model for events such as a breach, intrusion, attack, or incident. You will also be able to analyze an Advanced Persistent Threat (APT).

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.

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.

It is difficult to identify an adversary during the first stages of a cyberattack. Utilizing data collected from an incident or breach, signatures, and other relevant information can help you determine who the adversary might be.

Adversary Operator is the “hacker” or person(s) conducting the intrusion activity.

Adversary Customer is the entity that stands to benefit from the activity conducted in the intrusion. It may be the same person who stands behind the adversary operator, or it may be a separate person or group.

As an example, an adversary customer could control different operators simultaneously. Each operator might have its capabilities and infrastructure.

Victim

Victim – is a target of the adversary. A victim can be an organization, person, target email address, IP address, domain, etc. It's essential to understand the difference between the victim persona and the victim assets because they serve different analytic functions.

A victim can be an opportunity for the attackers to get a foothold on the organisation 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.

Victim Personae are the people and organizations being targeted and whose assets are being attacked and exploited. These can be organization names, people's names, industries, job roles, interests, etc.

Victim Assets are the attack surface and include the set of systems, networks, email addresses, hosts, IP addresses, social networking accounts, etc., to which the adversary will direct their capabilities.

Capability

Capability – is also known as 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 of 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.

An adversary must have the required capabilities. The capabilities can be malware and phishing email development skills or, at least, access to capabilities, such as acquiring malware or ransomware as a service.

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. For example, a command and control centre (C2) and the results from the victim (data exfiltration).

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.

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.

Event Meta Features

Six 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 don't occur in two or more events rather than just one. A great example can be the Cyber Kill Chain developed by Lockheed Martin.
  The phases can be:
  \1. Reconnaissance
  \2. Weaponization
  \3. Delivery
  \4. Exploitation
  \5. Installation
  \6. Command & Control
  \7. 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, virtualisation 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

Introduction to MITRE

For those that are new to the cybersecurity field, you probably never heard of MITRE. Those of us that have been around *might* only associate MITRE with CVEs (**Common Vulnerabilities and Exposures**) list, which is one resource you'll probably check when searching for an exploit for a given vulnerability. But MITRE researches in many areas, outside of cybersecurity, for the 'safety, stability, and well-being of our nation.' These areas include artificial intelligence, health informatics, space security, to name a few.

From **Mitre.org**: "*At MITRE, we solve problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation.*"

In this room, we will focus on other projects/research that the US-based non-profit MITRE Corporation has created for the cybersecurity community, specifically:

- ATT&CK® (**A**dversarial **T**actics, **T**echniques, **and C**ommon **K**nowledge) Framework
- CAR (**C**yber **A**nalytics **R**epository) Knowledge Base
- ENGAGE (sorry, not a fancy acronym)
- D3FEND (**D**etection, **D**enial, and **D**isruption **F**ramework **E**mpowering **N**etwork **D**efense)
- AEP (**A**TT&CK **E**mulation **P**lans)

Basic Terminology

Before diving in, let's briefly discuss a few terms that you will often hear when dealing with the framework, threat intelligence, etc.

APT is an acronym for **A***dvanced Persistent Threat*. **This can be considered a team/group (**threat group*****), or even country (***nation-state group*****), that engages in long-term attacks against organizations and/or countries. The term 'advanced' can be misleading as it will tend to cause us to believe that each APT group all have some super-weapon, e.i. a zero-day exploit, that they use. That is not the case. As we will see a bit later, the techniques these APT groups use are quite common and can be detected with the right implementations in place. You can view FireEye's current list of APT groups [**here**](https://www.fireeye.com/current-threats/apt-groups.html).

TTP is an acronym for **Tactics, Techniques, and Procedures,** but what does each of these terms mean?

- The **Tactic** is the adversary's goal or objective.
- The **Technique** is how the adversary achieves the goal or objective.
- The **Procedure** is how the technique is executed.

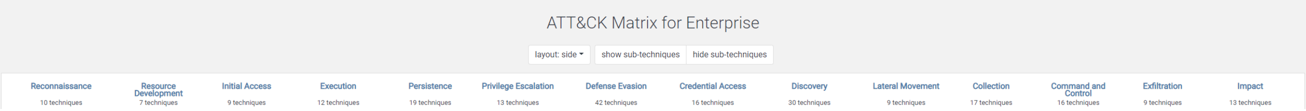
ATT&CK Framework

What is the ATT&CK® framework? According to the **website**, "MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations." In 2013, MITRE began to address the need to record and document common TTPs (**Tactics, Techniques, and Procedures**) that APT (**Advanced Persistent Threat**) groups used against enterprise Windows networks. This started with an internal project known as FMX (**Fort Meade Experiment**). Within this project, selected security professionals were tasked to emulated adversarial TTPs against a network, and data was collected from the attacks on this network. The gathered data helped construct the beginning pieces of what we know today as the ATT&CK® framework.

The ATT&CK® framework has grown and expanded throughout the years. One notable expansion was that the framework focused solely on the Windows platform but has expanded to cover other platforms, such as macOS and Linux. The framework is heavily contributed to by many sources, such as security researchers and threat intelligence reports. Note this is not only a tool for blue teamers. The tool is also useful for red teamers.

If you haven't done so, navigate to the ATT&CK® **website**.

Direct your attention to the bottom of the page to view the **ATT&CK® Matrix for Enterprise**. Across the top of the matrix, there are 14 categories. Each category contains the techniques an adversary could use to perform the tactic. The categories cover the seven-stage Cyber Attack Lifecycle (credit Lockheed Martin for the Cyber Kill Chain).

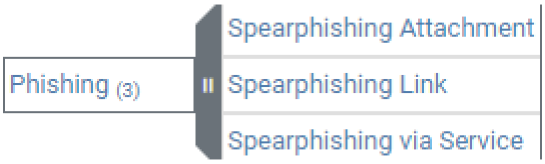


ATT&CK Matrix for Enterprise

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	7 techniques	9 techniques	12 techniques	19 techniques	13 techniques	42 techniques	16 techniques	30 techniques	9 techniques	17 techniques	16 techniques	9 techniques	13 techniques

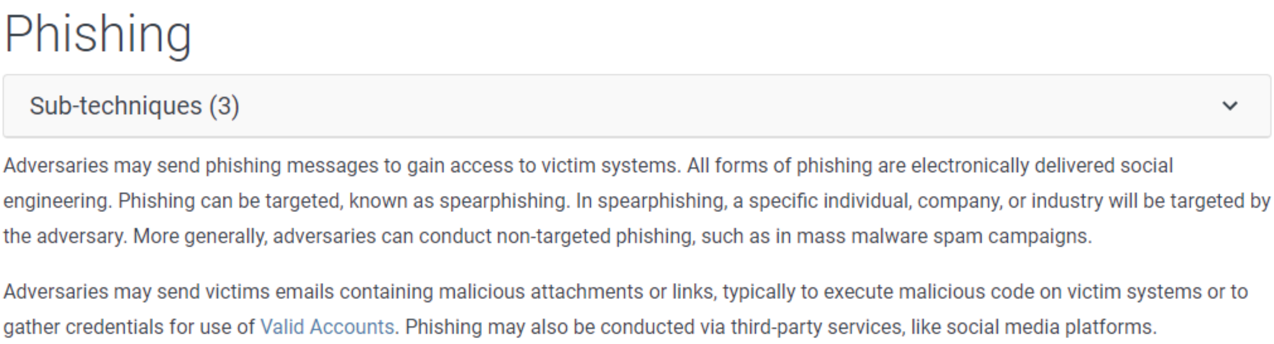
Under **Initial Access**, there are 9 techniques. Some of the techniques have sub-techniques, such as Phishing.

If we click on the gray bar to the right, a new layer appears listing the sub-techniques.



To get a better understanding of this technique and it's associated sub-techniques, click on Phishing.

We have been directed to a page dedicated to the technique known as Phishing and all related information regarding the technique, such as a brief description, **Procedure Examples**, and **Mitigations**.

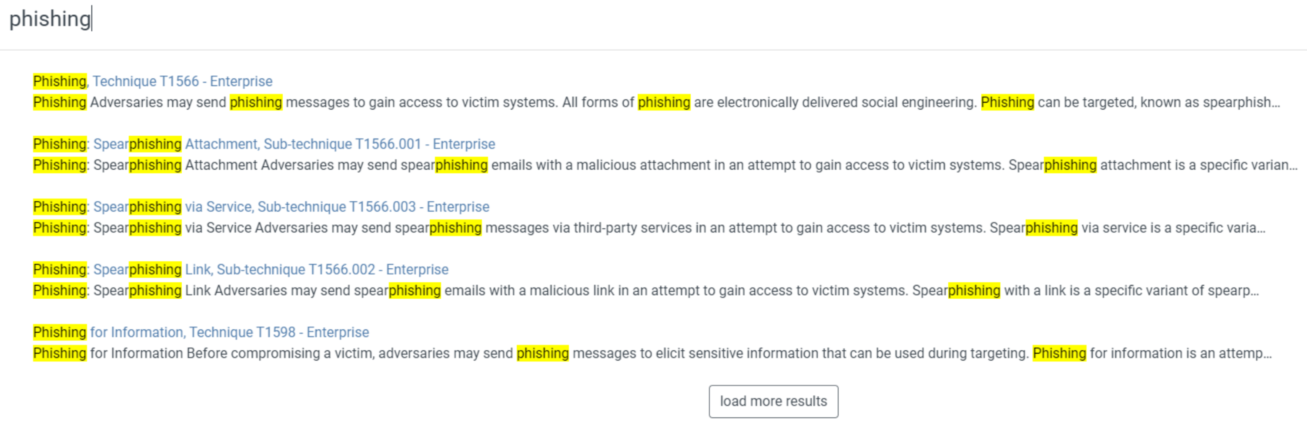


Phishing

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems or to gather credentials for use of Valid Accounts. Phishing may also be conducted via third-party services, like social media platforms.

You can alternatively resort to using the Search feature to retrieve all associated information regarding a given technique, sub-technique, and/or group.



phishing

Phishing, Technique T1566 - Enterprise
Phishing Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphish...

Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise
Phishing: Spearphishing Attachment Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific varian...

Phishing: Spearphishing via Service, Sub-technique T1566.003 - Enterprise
Phishing: Spearphishing via Service Adversaries may send spearphishing messages via third-party services in an attempt to gain access to victim systems. Spearphishing via service is a specific varia...

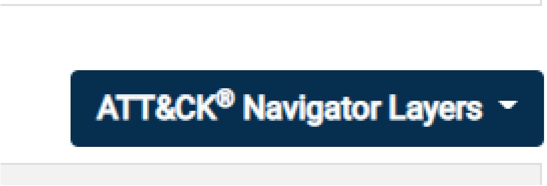
Phishing: Spearphishing Link, Sub-technique T1566.002 - Enterprise
Phishing: Spearphishing Link Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearp...

Phishing for Information, Technique T1598 - Enterprise
Phishing for Information Before compromising a victim, adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attemp...

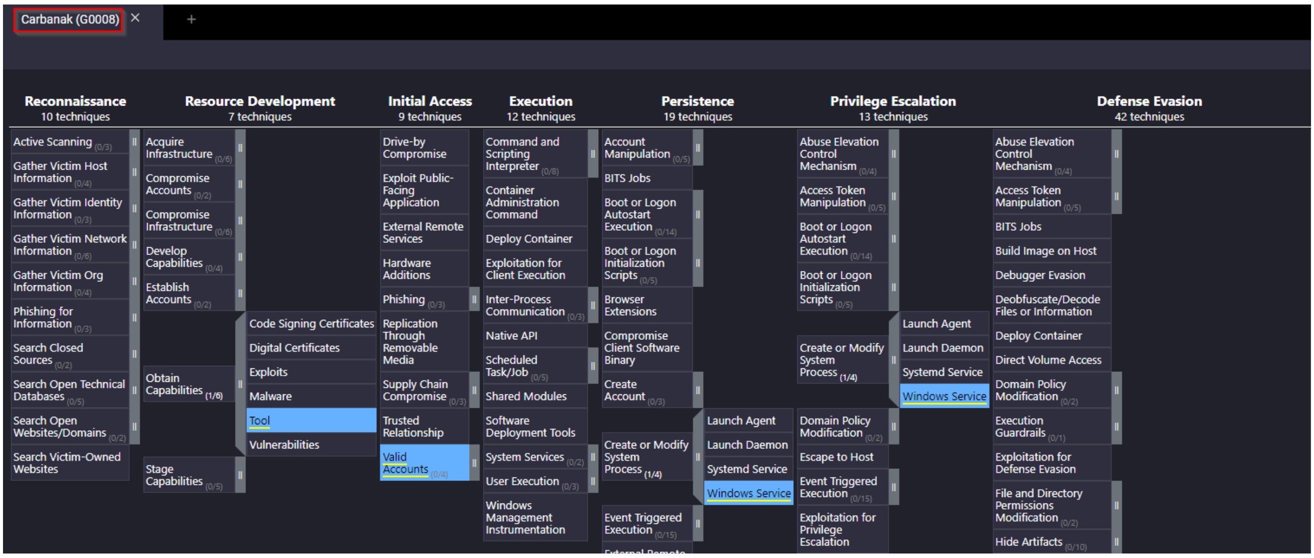
load more results

Lastly, 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*."

You can access the Navigator view when visiting a group or tool page. The ATT&CK® Navigator Layers button will be available.



In the sub-menu select **view**.

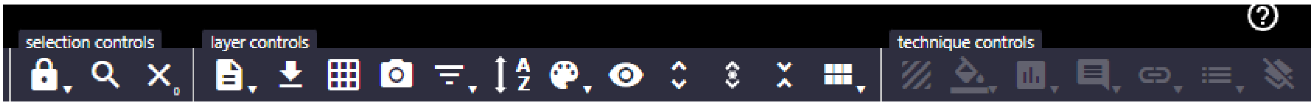


Carbanak (G0008)

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques
Active Scanning (0/3) Gather Victim Host Information (0/4) Gather Victim Identity Information (0/3) Gather Victim Network Information (0/6) Gather Victim Org Information (0/4) Phishing for Information (0/3) Search Closed Sources (0/2) Search Open Technical Databases (0/5) Search Open Websites/Domains (0/2) Search Victim-Owned Websites	Acquire Infrastructure (0/6) Compromise Accounts (0/2) Compromise Infrastructure (0/6) Develop Capabilities (0/4) Establish Accounts (0/2) Obtain Capabilities (1/6) Code Signing Certificates Digital Certificates Exploits Malware Tool Vulnerabilities Stage Capabilities (0/5)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (0/3) Replication Through Removable Media Supply Chain Compromise (0/3) Trusted Relationship Valid Accounts (0/4)	Command and Scripting Interpreter (0/8) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (0/3) Native API Scheduled Task/Job (0/5) Shared Modules Software Deployment Tools System Services (0/2) User Execution (0/3) Windows Management Instrumentation	Account Manipulation (0/5) BITS Jobs Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/5) Browser Extensions Compromise Client Software Binary Create Account (0/3) Create or Modify System Process (1/4) Launch Agent Launch Daemon Systemd Service Windows Service Event Triggered Execution (0/15) External Remote	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) Boot or Logon Autostart Execution (0/14) Boot or Logon Initialization Scripts (0/5) Create or Modify System Process (1/4) Launch Agent Launch Daemon Systemd Service Windows Service Domain Policy Modification (0/2) Escape to Host Event Triggered Execution (0/15) Exploitation for Privilege Escalation	Abuse Elevation Control Mechanism (0/4) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (0/2) Execution Guardrails (0/1) Exploitation for Defense Evasion File and Directory Permissions Modification (0/2) Hide Artifacts (0/10)

Let's get acquainted with this tool. Click **here** to view the ATT&CK® Navigator for Carbanak.

At the top left, there are 3 sets of controls: **selection controls**, **layer controls**, and **technique controls**. I encourage you to inspect each of the options under each control to get familiar with them. The question mark at the far right will provide additional information regarding the navigator.



To summarize, we can use the ATT&CK Matrix to map a threat group to their tactics and techniques. There are various methods the search can be initiated.

The questions below will help you become more familiar with the ATT&CK®. It is recommended to start answering the questions from the **Phishing page**. Note, that this link is for version 8 of the ATT&CK Matrix.

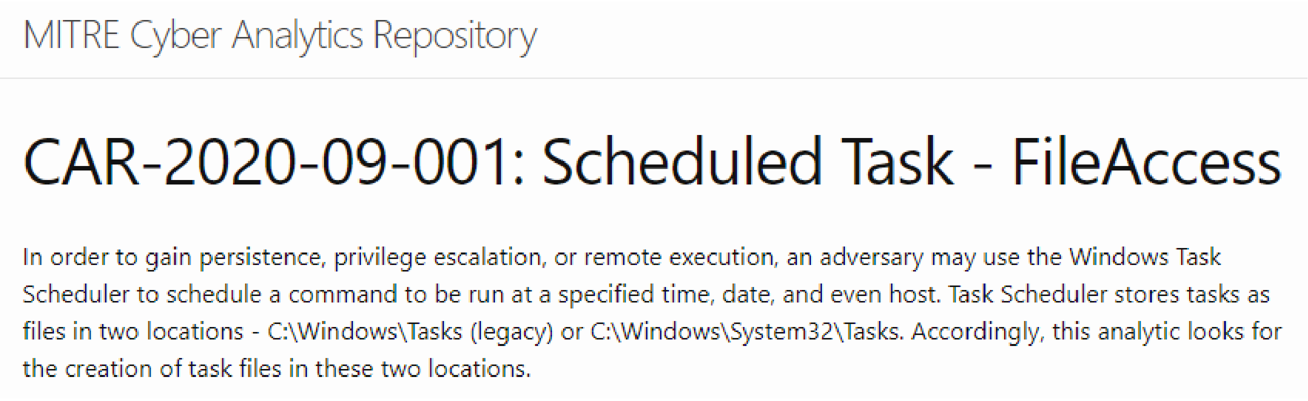
CAR Analytics Repository

The official definition of **CAR** is "*The MITRE 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. With respect to coverage, CAR is focused on providing a set of validated and well-explained analytics, in particular with regards to their operating theory and rationale.*"

Instead of further attempting to explain what CAR is, let's dive in. With our newly acquired knowledge from the previous section, we should feel comfortable and understand the information that CAR is providing to us.

Let's begin our journey by reviewing **CAR-2020-09-001: Scheduled Task - File Access**.

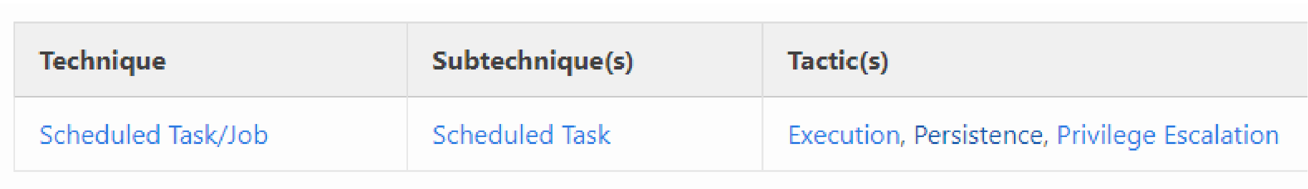
Upon visiting the page, we're given a brief description of the analytic and references to ATT&CK (**technique**, **sub-technique**, and **tactic**).



MITRE Cyber Analytics Repository

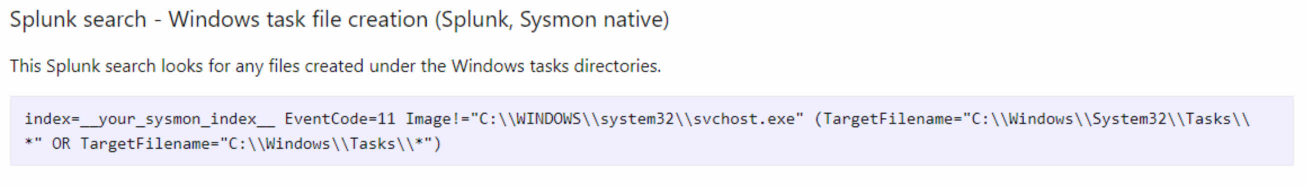
CAR-2020-09-001: Scheduled Task - FileAccess

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.



Technique	Subtechnique(s)	Tactic(s)
Scheduled Task/Job	Scheduled Task	Execution, Persistence, Privilege Escalation

We're also provided with Pseudocode and a query on how to search for this specific analytic within Splunk. A pseudocode is a plain, human-readable way to describe a set of instructions or algorithms that a program or system will perform.



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

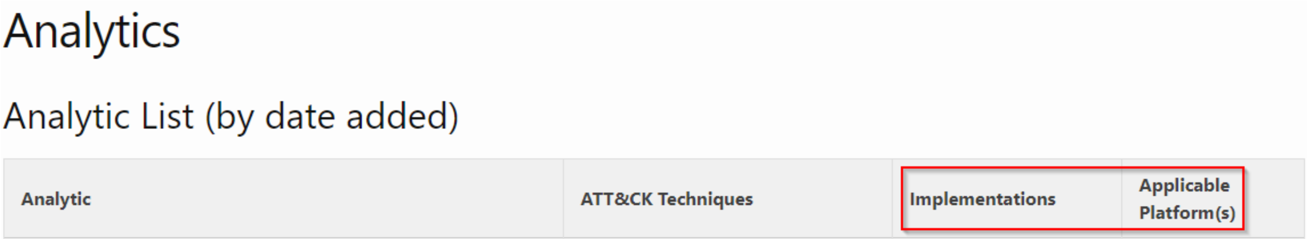
This Splunk search looks for any files created under the Windows tasks directories.

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

Note the reference to Sysmon. If you're not familiar with Sysmon, check out the Sysmon room.

To take full advantage of CAR, we can view the **Full Analytic List** or the **CAR ATT&CK® Navigator layer** to view all the analytics.

Full Analytic List



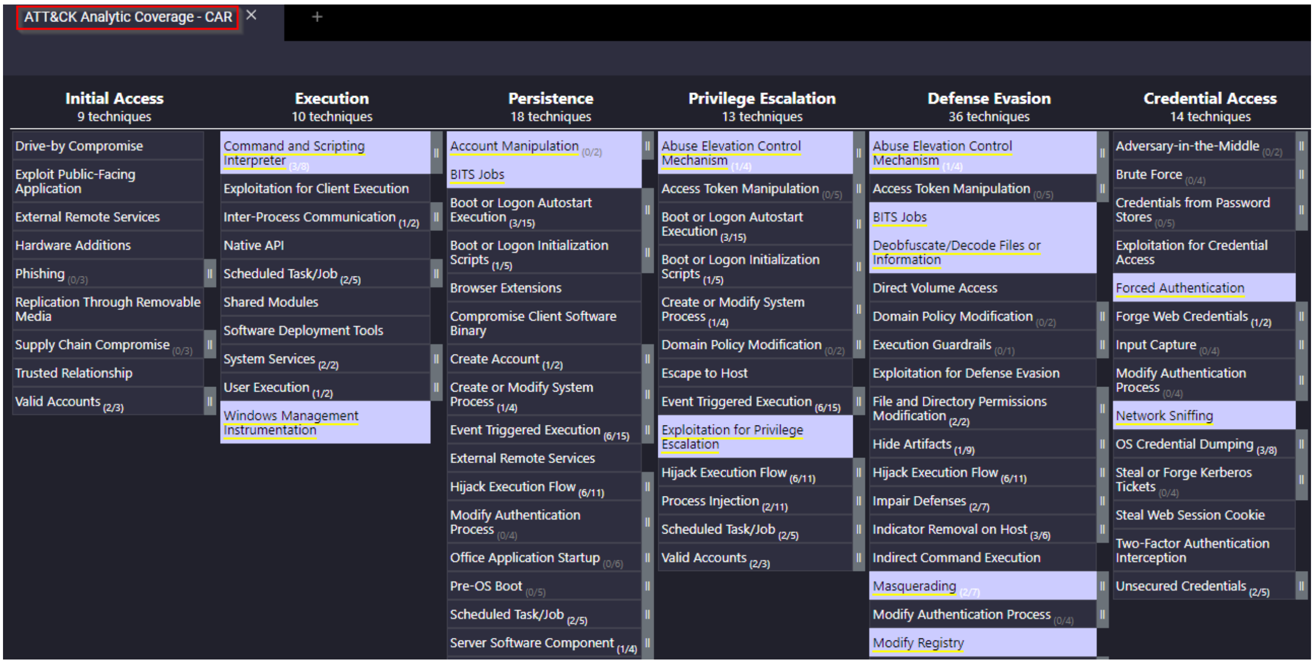
Analytics

Analytic List (by date added)

Analytic	ATT&CK Techniques	Implementations	Applicable Platform(s)

In the Full Analytic List view, we can see what implementations are available for any given analytic at a single glance, along with what OS platform it applies to.

CAR ATTACK Navigator



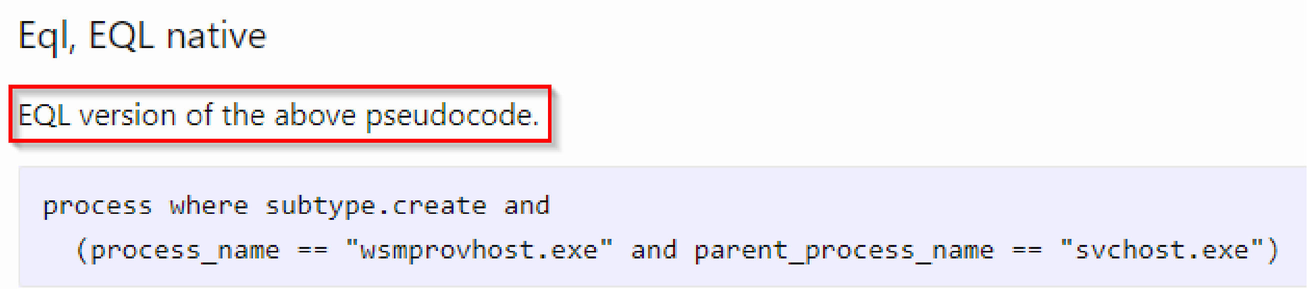
ATT&CK Analytic Coverage - CAR

Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 36 techniques	Credential Access 14 techniques
Drive-by Compromise	Command and Scripting Interpreter (3/8)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (1/4)	Abuse Elevation Control Mechanism (1/4)	Adversary-in-the-Middle (0/2)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
External Remote Services	Inter-Process Communication (1/2)	Boot or Logon Autostart Execution (3/15)	Boot or Logon Autostart Execution (3/15)	BITS Jobs	Credentials from Password Stores (0/5)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (1/5)	Boot or Logon Initialization Scripts (1/5)	Deobfuscate/Decode Files or Information	Exploitation for Credential Access
Phishing (0/3)	Scheduled Task/Job (2/5)	Browser Extensions	Create or Modify System Process (1/4)	Direct Volume Access	Forced Authentication
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (0/2)	Domain Policy Modification (0/2)	Forge Web Credentials (1/2)
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (1/2)	Escape to Host	Execution Guardrails (0/1)	Input Capture (0/4)
Trusted Relationship	System Services (2/2)	Create or Modify System Process (1/4)	Event Triggered Execution (6/15)	Exploitation for Defense Evasion	Modify Authentication Process (0/4)
Valid Accounts (2/3)	User Execution (1/2)	Event Triggered Execution (6/15)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2/2)	Network Sniffing
	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (6/11)	Hide Artifacts (1/9)	OS Credential Dumping (3/8)
		Hijack Execution Flow (6/11)	Process Injection (2/11)	Hijack Execution Flow (6/11)	Steal or Forge Kerberos Tickets (0/4)
		Modify Authentication Process (0/4)	Scheduled Task/Job (2/5)	Impair Defenses (2/7)	Steal Web Session Cookie
		Office Application Startup (0/6)	Valid Accounts (2/3)	Indicator Removal on Host (3/6)	Two-Factor Authentication Interception
		Pre-OS Boot (0/5)		Indirect Command Execution	Unsecured Credentials (2/5)
		Scheduled Task/Job (2/5)		Masquerading (2/7)	
		Server Software Component (1/4)		Modify Authentication Process (0/4)	
				Modify Registry	

(The techniques highlighted in purple are the analytics currently in CAR)

Let's look at another analytic to see a different implementation, **CAR-2014-11-004: Remote PowerShell Sessions**.

Under Implementations, a pseudocode is provided and an EQL version of the pseudocode. EQL (pronounced as 'equal'), and it's an acronym for Event Query Language. EQL can be utilized to query, parse, and organize Sysmon event data. You can read more about this **here**.



Eql, EQL native

EQL version of the above pseudocode.

```
process where subtype.create and
  (process_name == "wsmprovhost.exe" and parent_process_name == "svchost.exe")
```

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 ENGAGE

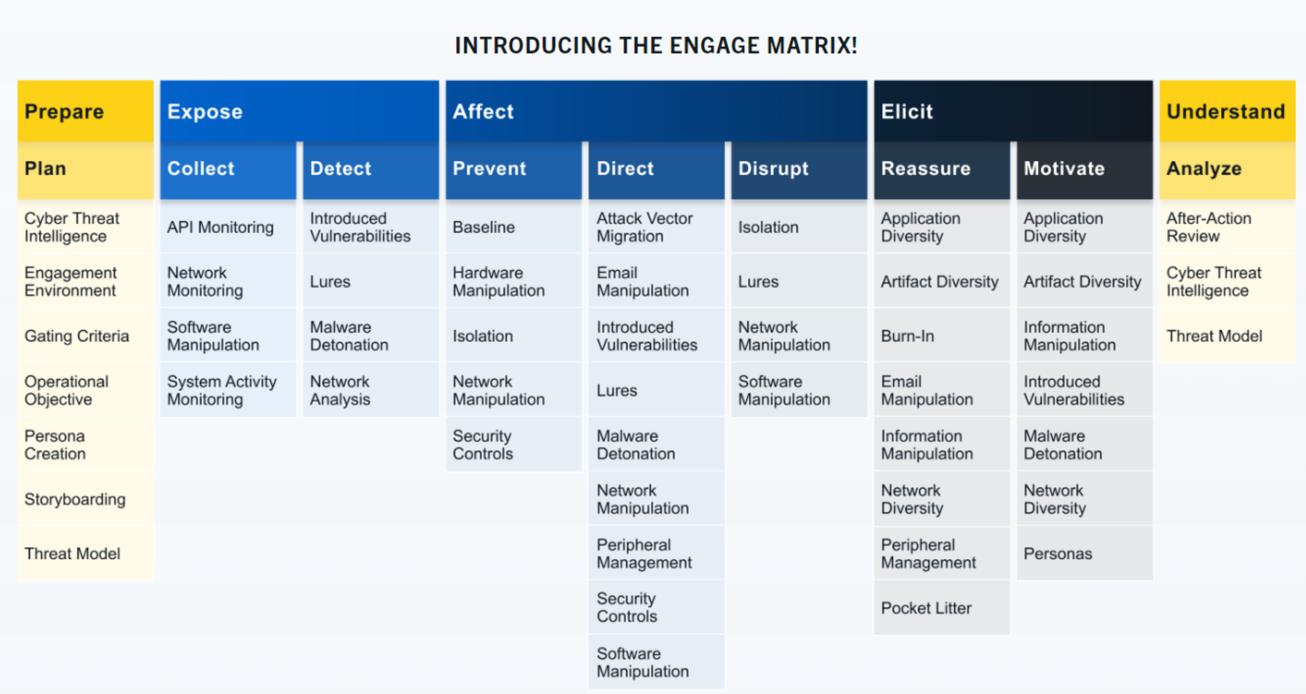
Per the website, "***MITRE Engage*** *is a framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals.*"

MITRE Engage is considered an **Adversary Engagement Approach**. This is accomplished by the implementation of **Cyber Denial** and **Cyber Deception**.

With **Cyber Denial** we prevent the adversary's ability to conduct their operations and with **Cyber Deception** we intentionally plant artifacts to mislead the adversary.

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.

As with MITRE ATT&CK, Engage has its own matrix. Below is a visual of the **Engage Matrix**.



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				

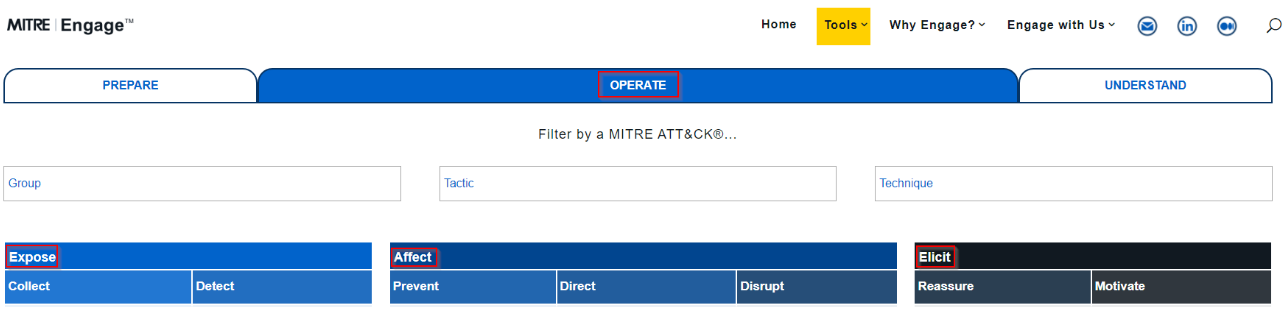
Let's quickly explain each of these categories based on the information on the Engage website.

- **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)

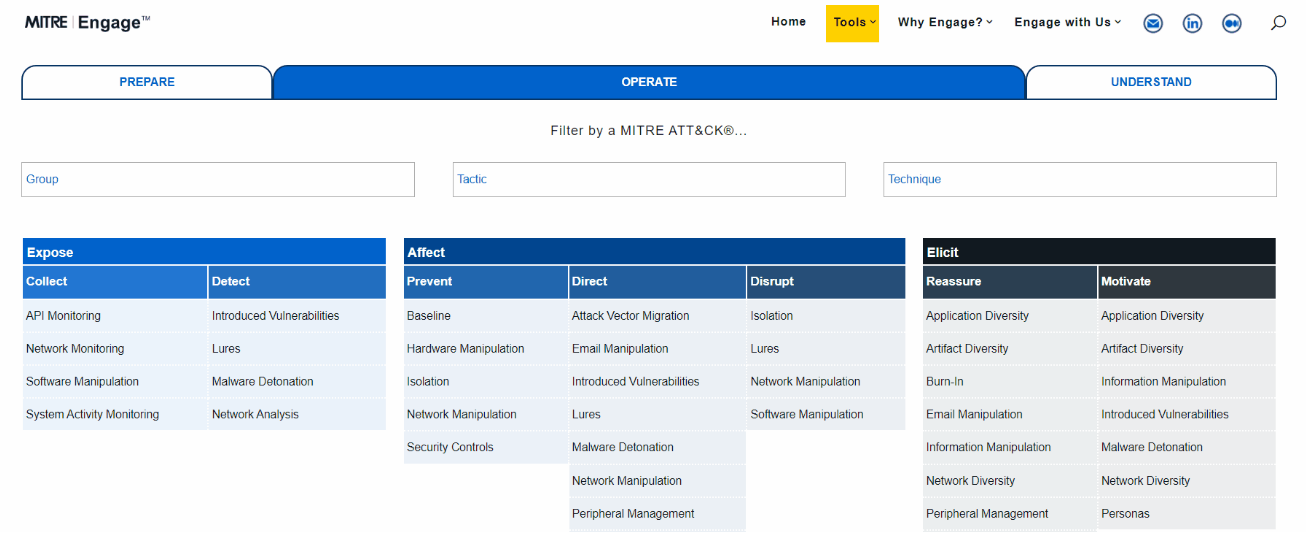
Refer to the Engage Handbook to learn more.

You can interact with the Engage Matrix Explorer. We can filter by information from **MITRE ATT&CK**.

Note that by default the matrix focuses on **Operate**, which entails **Expose**, **Affect**, and **Elicit**.



You can click on **Prepare** or **Understand** if you wish to focus solely on that part of the matrix.



MITRE | Engage™

PREPARE | OPERATE | UNDERSTAND

Filter by a MITRE ATT&CK®...

Group | Tactic | Technique

Expose		Affect			Elicit	
Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate
API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity
Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity
Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation
System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities
		Security Controls	Malware Detonation		Information Manipulation	Malware Detonation
			Network Manipulation		Network Diversity	Network Diversity
			Peripheral Management		Peripheral Management	Personas

That should be enough of an overview. We'll leave it to you to explore the resources provided to you on this website.

Before moving on, let's practice using this resource by answering the questions below.

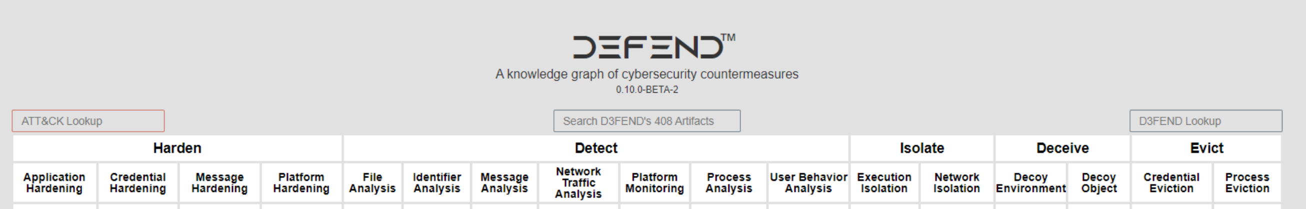
D3FEND

What is this MITRE resource? Per the **D3FEND** website, this resource is "*A knowledge graph of cybersecurity countermeasures.*"

D3FEND is still in beta and is funded by the Cybersecurity Directorate of the NSA.

D3FEND stands for **D**etection, **D**enial, and **D**isruption **F**ramework **E**mpowering **N**etwork **D**efense.

At the time of this writing, there are 408 artifacts in the D3FEND matrix. See the below image.



D3FEND™

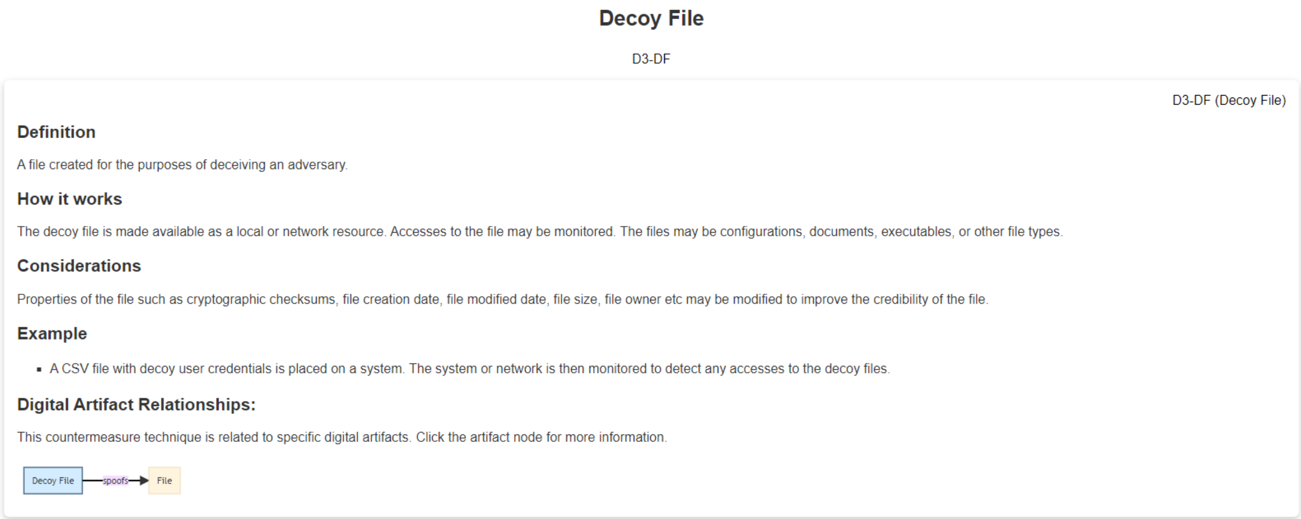
A knowledge graph of cybersecurity countermeasures

0.10.0-BETA-2

ATT&CK Lookup | Search D3FEND's 408 Artifacts | D3FEND Lookup

Harden				Detect								Isolate		Deceive		Evict	
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	Process Eviction

Let's take a quick look at one of the D3FENDs artifacts, such as **Decoy File**.



Decoy File

D3-DF

D3-DF (Decoy File)

Definition

A file created for the purposes of deceiving an adversary.

How it works

The decoy file is made available as a local or network resource. Accesses to the file may be monitored. The files may be configurations, documents, executables, or other file types.

Considerations

Properties of the file such as cryptographic checksums, file creation date, file modified date, file size, file owner etc may be modified to improve the credibility of the file.

Example

- A CSV file with decoy user credentials is placed on a system. The system or network is then monitored to detect any accesses to the decoy files.

Digital Artifact Relationships:

This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

As you can see, 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.

The objective of this task is to make you aware of this MITRE resource and hopefully you'll keep an eye on it as it matures in the future.

We will still encourage you to navigate the website a bit by answering the questions below.

ATT&CK® Emulation

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

CTID

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 defense for all.

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

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

Per the website, "*Together with Participant organizations, we cultivate solutions for a safer world and advance threat-informed defense with open-source software, methodologies, and frameworks. By expanding upon the MITRE ATT&CK knowledge base, our work expands the global understanding of cyber adversaries and their tradecraft with the public release of data sets critical to better understanding adversarial behavior and their movements.*"

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 the 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.

Review the emulation plans to answer the questions below.

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.

Scenario: You are a security analyst who works in the aviation sector. Your organisation is moving their infrastructure to the cloud. Your goal is to use the ATT&CK® Matrix to gather threat intelligence on APT groups who might target this particular sector and use techniques targeting your areas of concern. You are checking to see if there are any gaps in coverage. After selecting a group, look over the selected group's information and their tactics, techniques, etc.

What is a group that targets your sector who has been in operation since at least 2013?

apt33

As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?

cloud accounts

What tool is associated with the technique from the previous question?

ruler

Per the detection tip, what should you be detecting? (format: phrase1 or phrase2)

abnoramal or malicious behavior

What platforms does the technique from question #2 affect?

Answer Azure AD, Google Workspace, IaaS, Office 365, SaaS