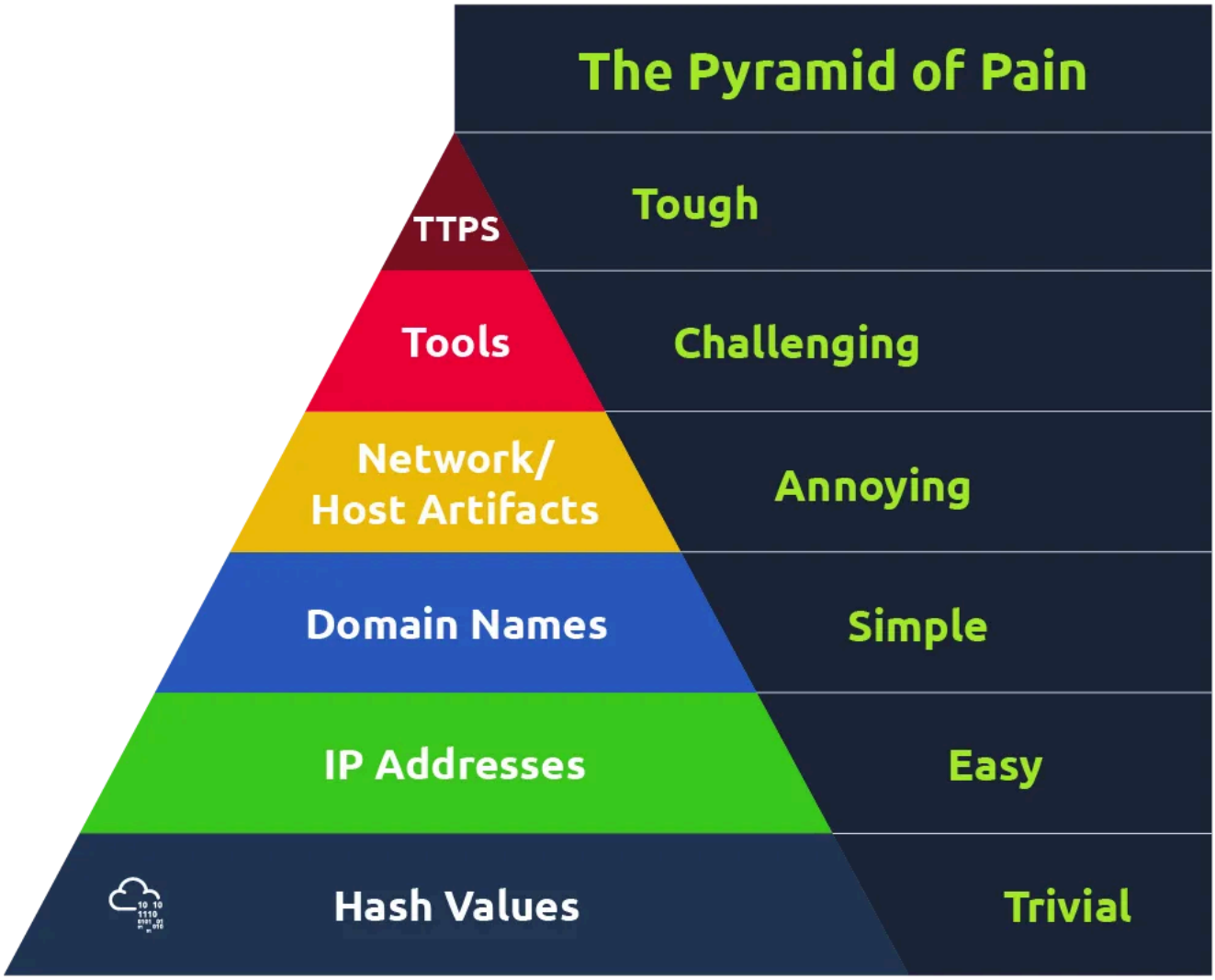
Pyramid Of Pain | SOC Level 1 | TryHackMe Walkthrough

Abhijeet Singh · Follow
12 min read · Jun 2, 2023

Task 1 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?

Answer the questions below

Task 2 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.

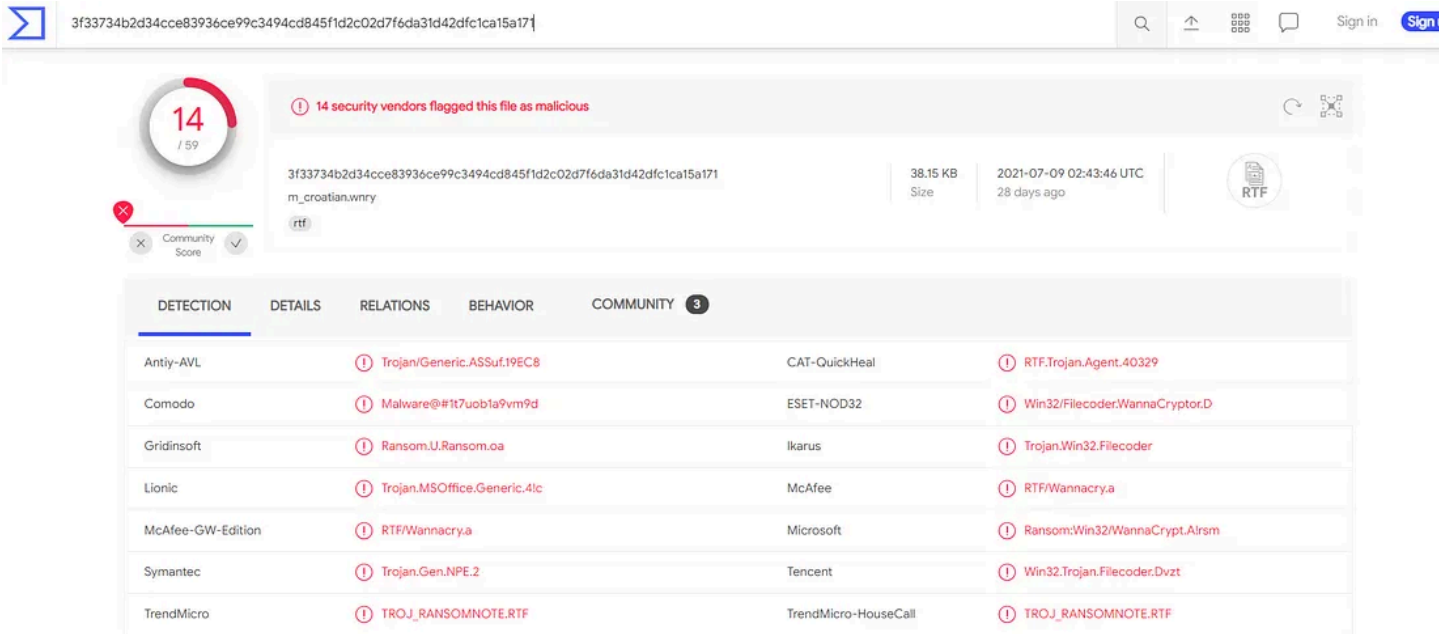
A hash is not considered to be cryptographically secure if two files have the same hash value or digest.

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've probably read 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.

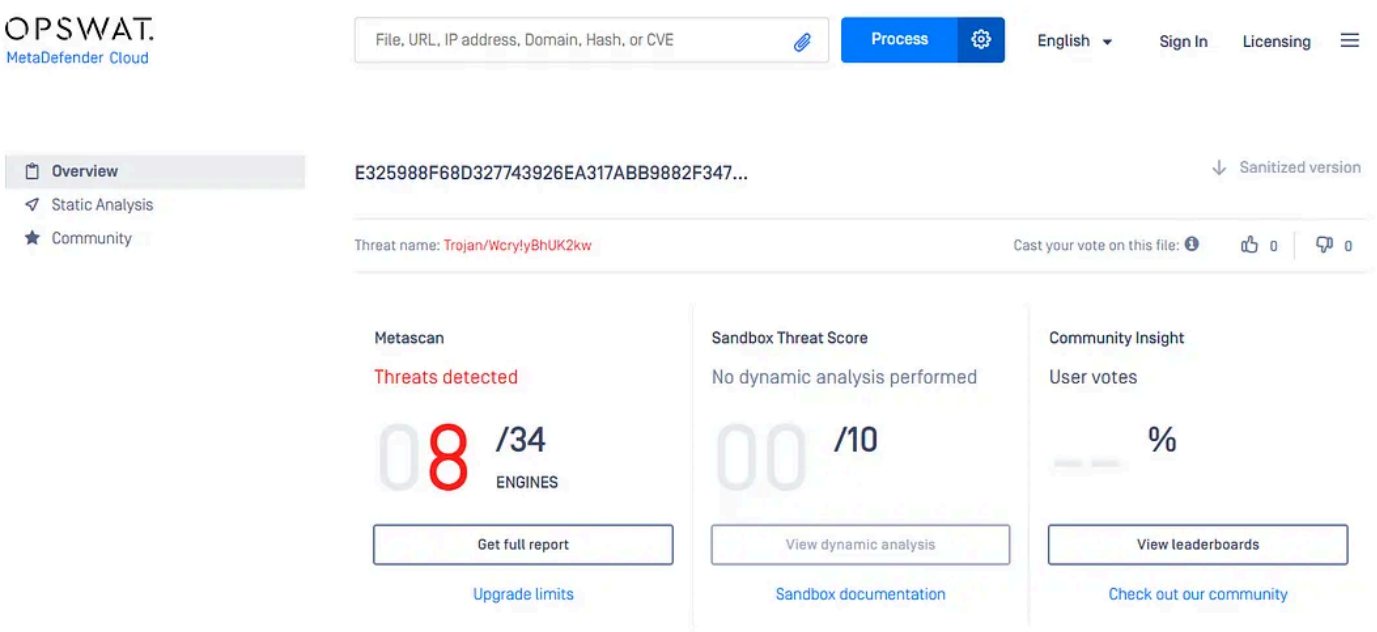
Various online tools can be used to do hash lookups like VirusTotal and Metadefender Cloud — OPSWAT.

VirusTotal:



Below the hash in the screenshot above, you can see the filename. In this case, it is "m_croetian.wnry"

MetaDefender Cloud — OPSWAT:



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, modifying a file by even a single bit is trivial, 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 difficult.

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 -Algorit
Algorithm Hash                                  Path
--------- ----                                  ----
MD5       D1A008E3A606F24590A02B853E955CF7 C:\Users\THM\Downloads\OpenVPN_2.5.1
```

File Hash (After Modification)

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

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

Answer the questions below

Analyse the report associated with the hash "b8ef959a9176aef07fdca8705254a163b50b49a17217a4ff0107487f59d4a35d" here. What is the filename of the sample?

Ans:- Sales_Receipt 5606.xls

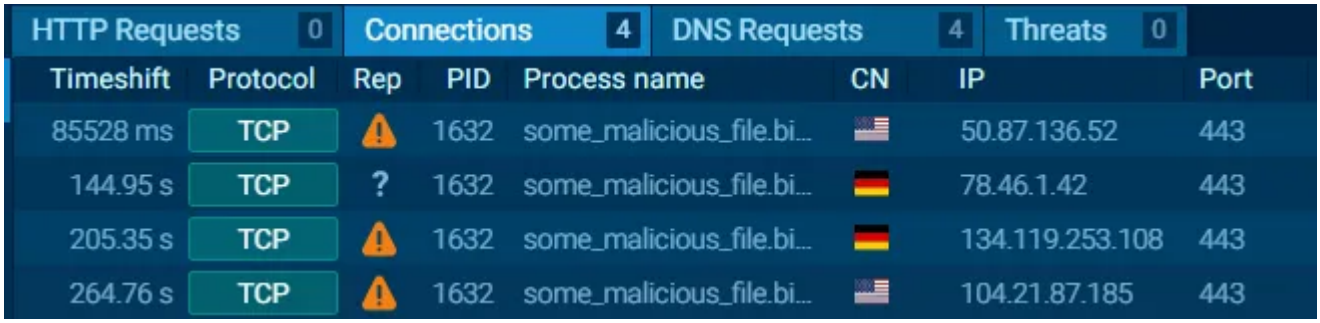
Task 3 IP Address (Easy)

You may have learned the importance of an IP Address from the "What is Networking?" Room. the importance of the IP Address. 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 defense standpoint, knowledge of the IP addresses an adversary uses can be valuable. A common defense tactic is to block, drop, or deny inbound requests from IP addresses on your parameter or external firewall. 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):



NOTE! Do not attempt to interact with the IP addresses shown above.

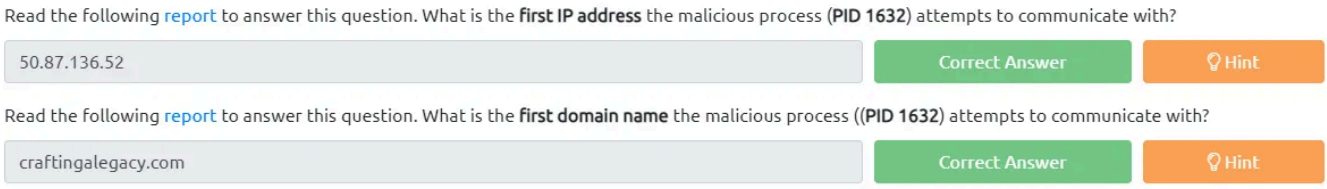
One of the ways an adversary can make it challenging to successfully carry out IP blocking is by using Fast Flux.

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"

Read the following report (generated from any.run) for this sample here to answer the questions below:

Answer the questions below



Task 4 Domain Names (Simple)

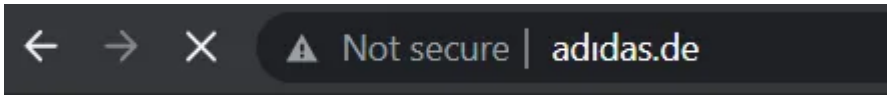
Let's step up the Pyramid of Pain and move on to Domain Names. You can see the transition of colors — from green to teal.

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). But we will not go into the details of how the Domain Name System (DNS) works. You can learn more about DNS in this "DNS in Detail" Room.

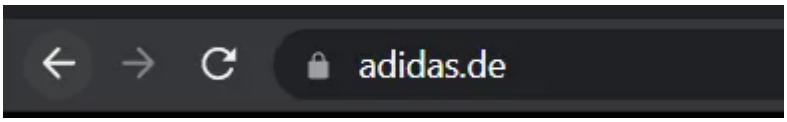
Domain Names can be a little more of a pain for the attacker to change as they would most likely need to purchase the domain, register it and modify DNS records. Unfortunately for defenders, many DNS providers have loose standards and provide APIs to make it even easier for the attacker to change the 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.

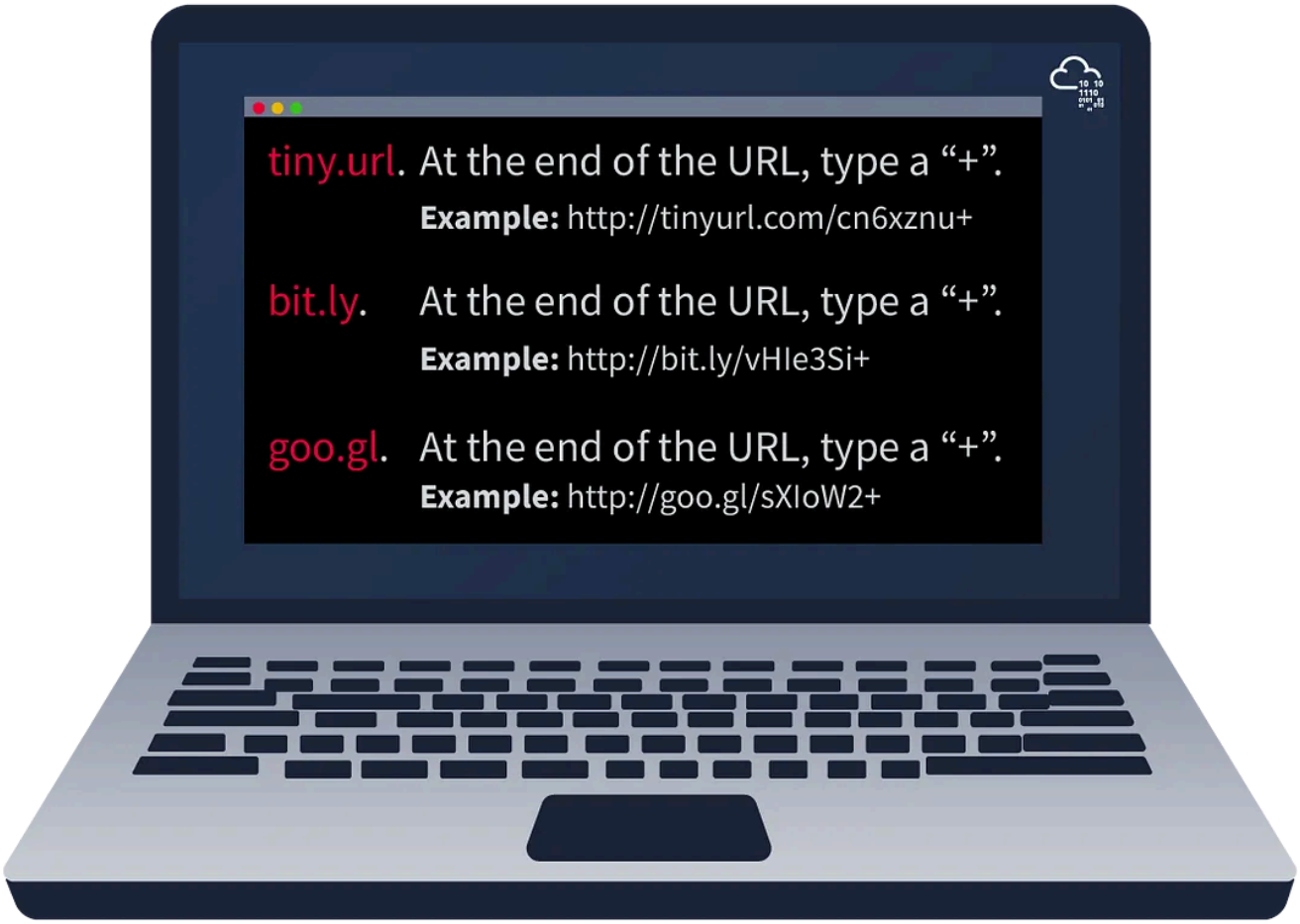
To detect the malicious domains, proxy logs or web server logs can be used.

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.

NOTE: The examples of the shortened links below are non-existent.



Viewing Domain Names in Any.run:

Answer the questions below

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

craftingalegacy.com — Correct Answer

What term refers to an address used to access websites?

Domain Name — Correct Answer

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

Punycode attack — Correct Answer

Provide the redirected website for the shortened URL using a preview: https://tinyurl.com/bw7t8p4u

https://tryhackme.com/ — Correct Answer

Task 5 Host Artifacts (Annoying)

Let’s take another step up to the yellow zone.

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	

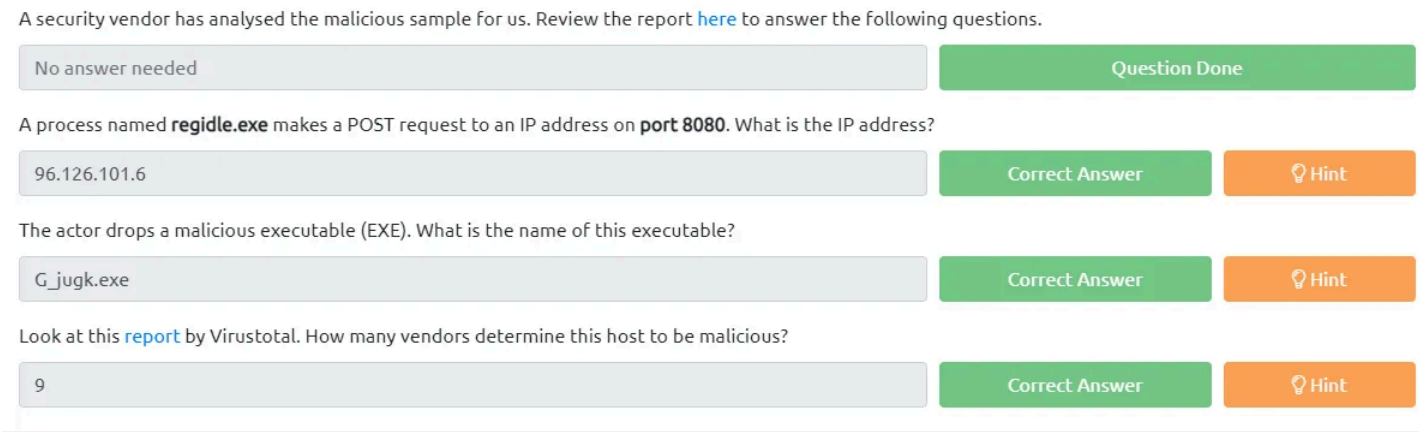
Suspicious events followed by opening a malicious application:

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:

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

Answer the questions below



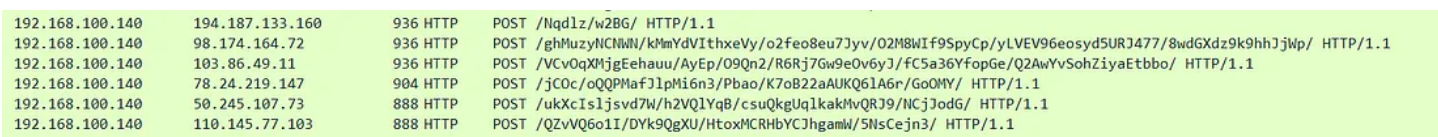
Task 6 Network Artifacts (Annoying)

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.

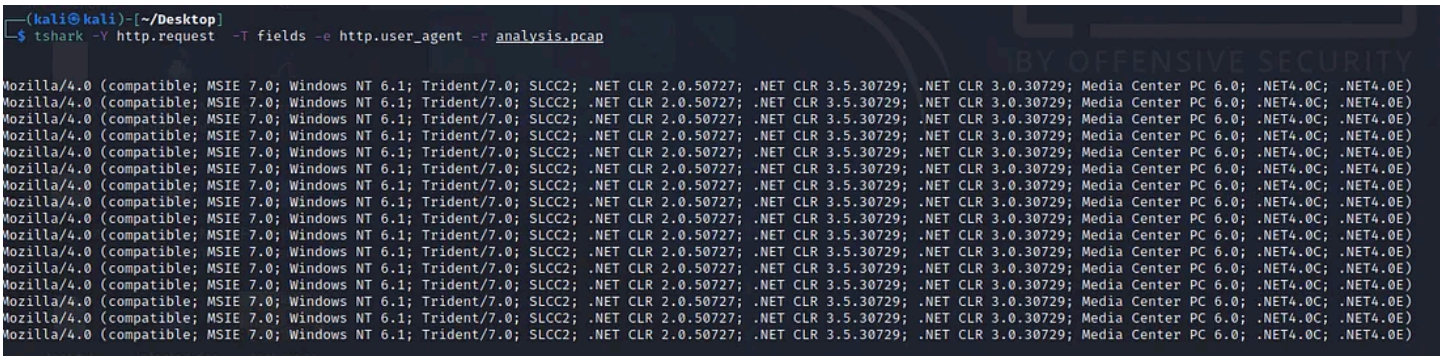
A network artifact can be a user-agent string, C2 information, or URI patterns followed by the HTTP POST requests.An attacker might use a User-Agent string that hasn't been observed in your environment before or seems out of the ordinary. The User-Agent is defined by RFC2616 as the request-header field 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 analyzer such as TShark or exploring IDS (Intrusion Detection System) logging from a source such as Snort.

HTTP POST requests containing suspicious strings:



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`



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.

Answer the questions below

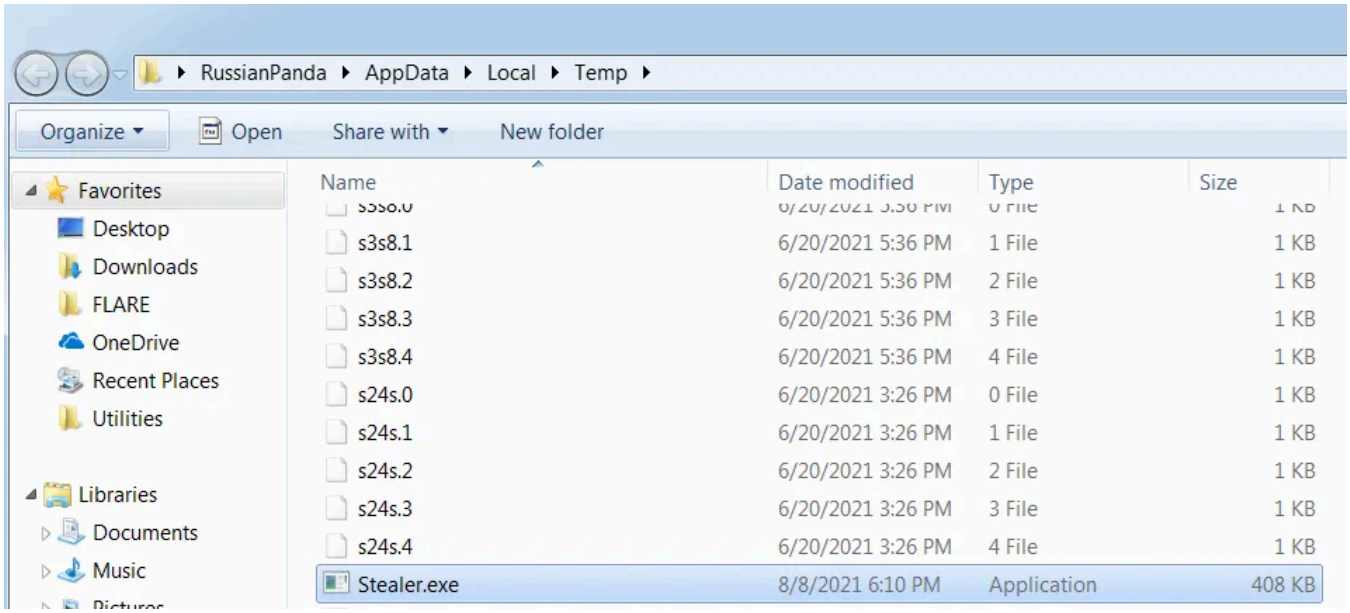
Task 7 Tools (Challenging)

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:



The execution of the suspicious binary:

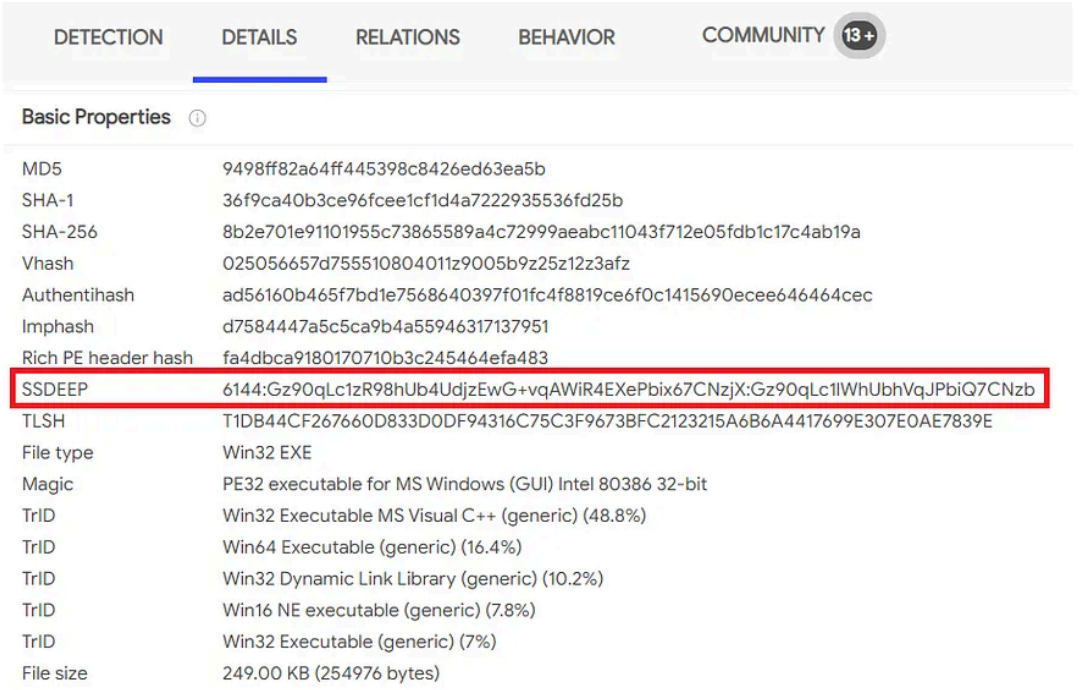
Antivirus signatures, detection rules, and YARA rules can be great weapons for you to use against attackers at this stage.

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.

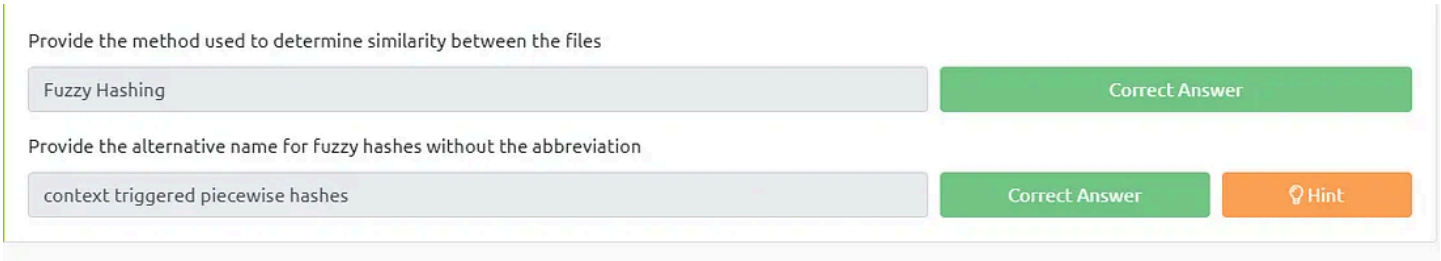
For detection rules, SOC Prime Threat Detection Marketplace is a great platform, where security professionals share their detection rules for different kinds of threats including the latest CVE's that are being exploited in the wild by adversaries.

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:



Answer the questions belo



Task 8 TTPs (Tough)

It is not over yet. But good news, we made it to the final stage or the apex of the Pyramid of Pain!

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.

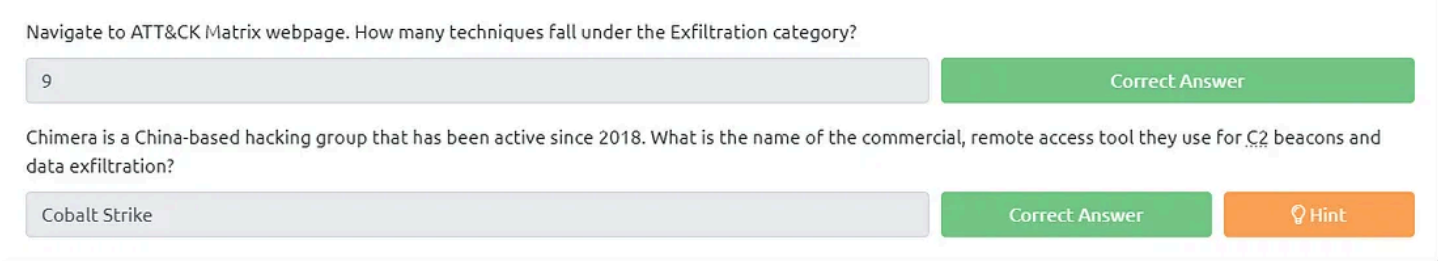
If you can detect and respond to the TTPs quickly, you leave the adversaries almost no chance to fight back. For, example if you could detect a Pass-the-Hash attack using Windows Event Log Monitoring and remediate it, you would be able to find the compromised host very quickly and stop the lateral movement 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.

Answer the questions below



Task 9 Practical: The Pyramid of Pain

Deploy the static site attached to this task and place the prompts into the correct tiers in the pyramid of pain!

Once you are sure, submit your answer on the static site to retrieve a flag!

Answer the questions below

Task 10 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?"

As David Blanco states, "*the amount of pain you cause an adversary depends on the types of indicators you are able to make use of*".

Answer the questions below

Read the above.

No answer needed

Question Done

Follow

Written by Abhijeet Singh

53 Followers · 18 Following

I am a passionate security researcher with a solid foundation and experience in networking and Linux.

Responses (1)

What are your thoughts?

Respond

Noah W
9 months ago

Plagiarism.

Not a walkthrough at all.

Reply

More from Abhijeet Singh

Abhijeet Singh

Advent of Cyber 2024 [Day 3] Even if I wanted to go, their vulnerabilities wouldn't allow it.

So, Let's Start with the Questions. I hope you already read the story and all the given instructions —

Dec 4, 2024 2

Abhijeet Singh

Advent of Cyber 2024 [Day 6] If I can’t find a nice malware to use, I’m not going.|

- Welcome to the Day 6 of the Advent of Cyber 2024 -

Dec 7, 2024

Abhijeet Singh

Advent of Cyber 2024 [Day 5] SOC-mas XX-what-ee? | TryHackMe Walkthrough

- Welcome to the Day 5 of the Advent of Cyber 2024 -

Dec 6, 2024

Abhijeet Singh

Advent of Cyber 2024 [Day 17] He analyzed and analyzed till his analyzer was sore!

-Welcome to the Day 17 of the Advent of Cyber 2024-

Dec 23, 2024

See all from Abhijeet Singh

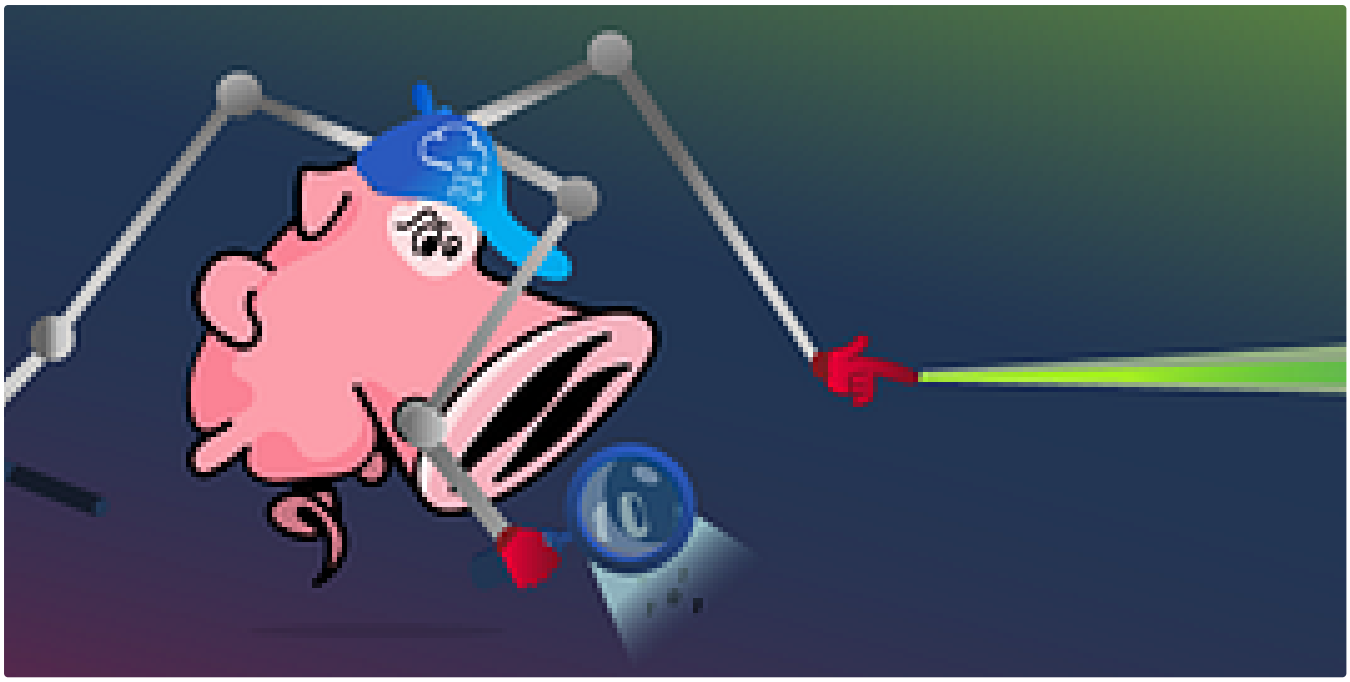
Recommended from Medium

Trnty

TryHackMe | Introduction To Honeypots Walkthrough

A guided room covering the deployment of honeypots and analysis of botnet activities

Sep 7, 2024 10



In T3CH by Axoloth

TryHackMe | Snort Challenge—The Basics | WriteUp

Put your snort skills into practice and write snort rules to analyse live capture network traffic

Nov 9, 2024 100

Lists

Staff picks

796 stories · 1558 saves

Stories to Help You Level-Up at Work

19 stories · 912 saves

Self-Improvement 101

20 stories · 3191 saves

Productivity 101

20 stories · 2704 saves

Abhijeet Singh

Advent of Cyber 2024 [Day 4] I'm all atomic inside! | TryHackMe Walkthrough

Please go through the story, Cyber Attacks, the Kill Chain and MITRE ATT&CK related content for better understanding of this room.

Dec 5, 2024 1

Abhijeet Singh

Advent of Cyber 2024 [Day 3] Even if I wanted to go, their vulnerabilities wouldn't allow it.

So, Let’s Start with the Questions. I hope you already read the story and all the given instructions —

Dec 4, 2024 2

Abhijeet Singh

Advent of Cyber 2024 [Day 8] Shellcodes of the world, unite! | TryHackMe Walkthrough

- Welcome to the Day 8 of the Advent of Cyber 2024 -

Dec 11, 2024

Abhijeet Singh

Advent of Cyber 2024 [Day 6] If I can’t find a nice malware to use, I’m not going.|

- Welcome to the Day 6 of the Advent of Cyber 2024 -

Dec 7, 2024

See more recommendations