



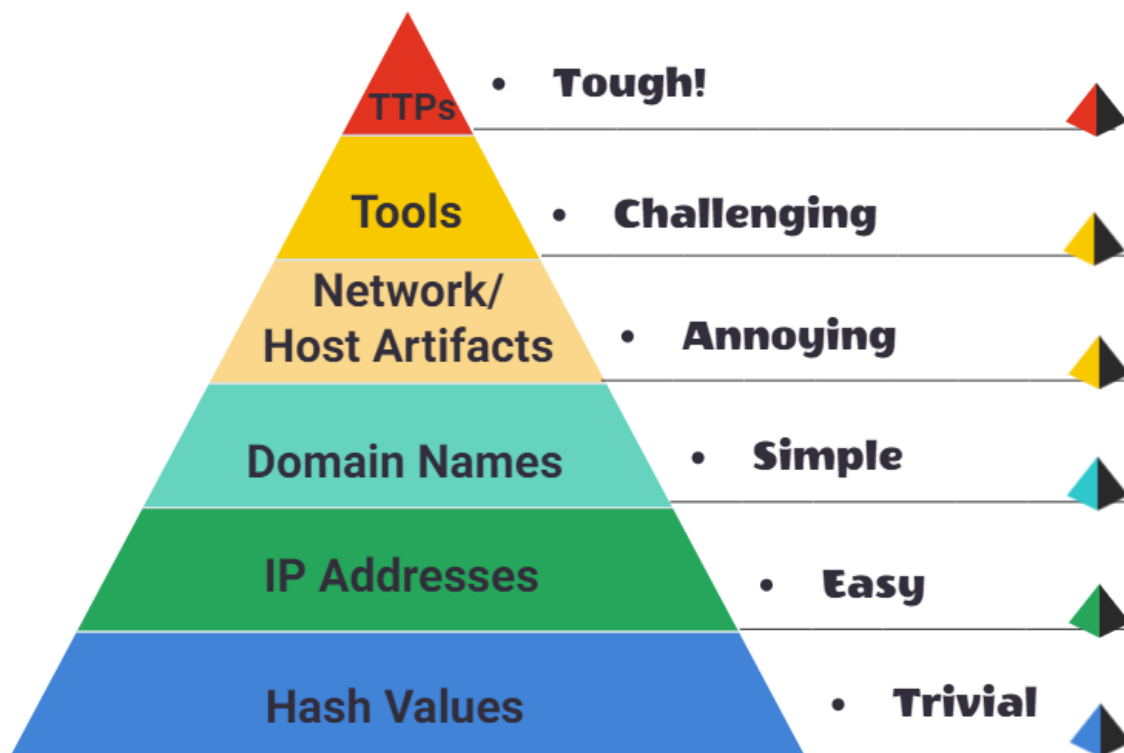
## Pyramid Of Pain

Learn what is the Pyramid of Pain and how to utilize this model to determine the level of difficulty it will cause for an adversary to change the indicators associated with them, and their campaign.

<https://tryhackme.com/room/pyramidofpainax>

### Task 1 Introduction

#### The Pyramid of Pain



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.

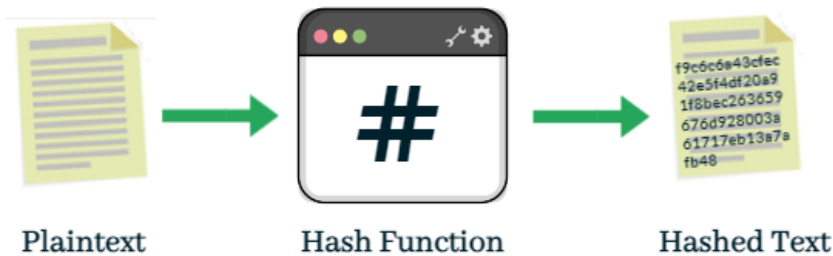
Understanding the Pyramid of Pain concept as a Threat Hunter, Incident Responder, or SOC Analyst is important.

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

Answer the questions below

Read the above.

## 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 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:**

14

/ 59

Community Score

✖

✔

14 security vendors flagged this file as malicious

3f33734b2d34cce83936ce99c3494cd845f1d2c02d7f6da31d42dfc1ca15a171

m\_croatian.wmry

rtf

38.15 KB

Size

2021-07-09 02:43:46 UTC

28 days ago

RTF

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 3

AntiY-AVL	<div>1</div> Trojan.Generic.ASuf.19EC8	CAT-QuickHeal	<div>1</div> RTF.Trojan.Agent.40329
Comodo	<div>1</div> Malware@#1t7uob1a9vm9d	ESET-NOD32	<div>1</div> Win32/Filecoder.WannaCryptor.D
Gridinsoft	<div>1</div> Ransom.U.Ransom.oa	Ikarus	<div>1</div> Trojan.Win32.Filecoder
Lionic	<div>1</div> Trojan.MSOffice.Generic.4lc	McAfee	<div>1</div> RTF/Wannacry.a
McAfee-GW-Edition	<div>1</div> RTF/Wannacry.a	Microsoft	<div>1</div> Ransom:Win32/WannaCrypt.Alrsm
Symantec	<div>1</div> Trojan.Gen.NPE.2	Tencent	<div>1</div> Win32.Trojan.Filecoder.Dvzt
TrendMicro	<div>1</div> TROJ_RANSOMNOTE.RTF	TrendMicro-HouseCall	<div>1</div> TROJ_RANSOMNOTE.RTF

## MetaDefender Cloud - OPSWAT:

OPSWAT.  
MetaDefender Cloud



English



☒ Overview

☐ Static Analysis

☐ Community

E325988F68D327743926EA317ABB9882F347...

Threat name: Trojan/WcrylyBhUK2kw




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
-----
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
```



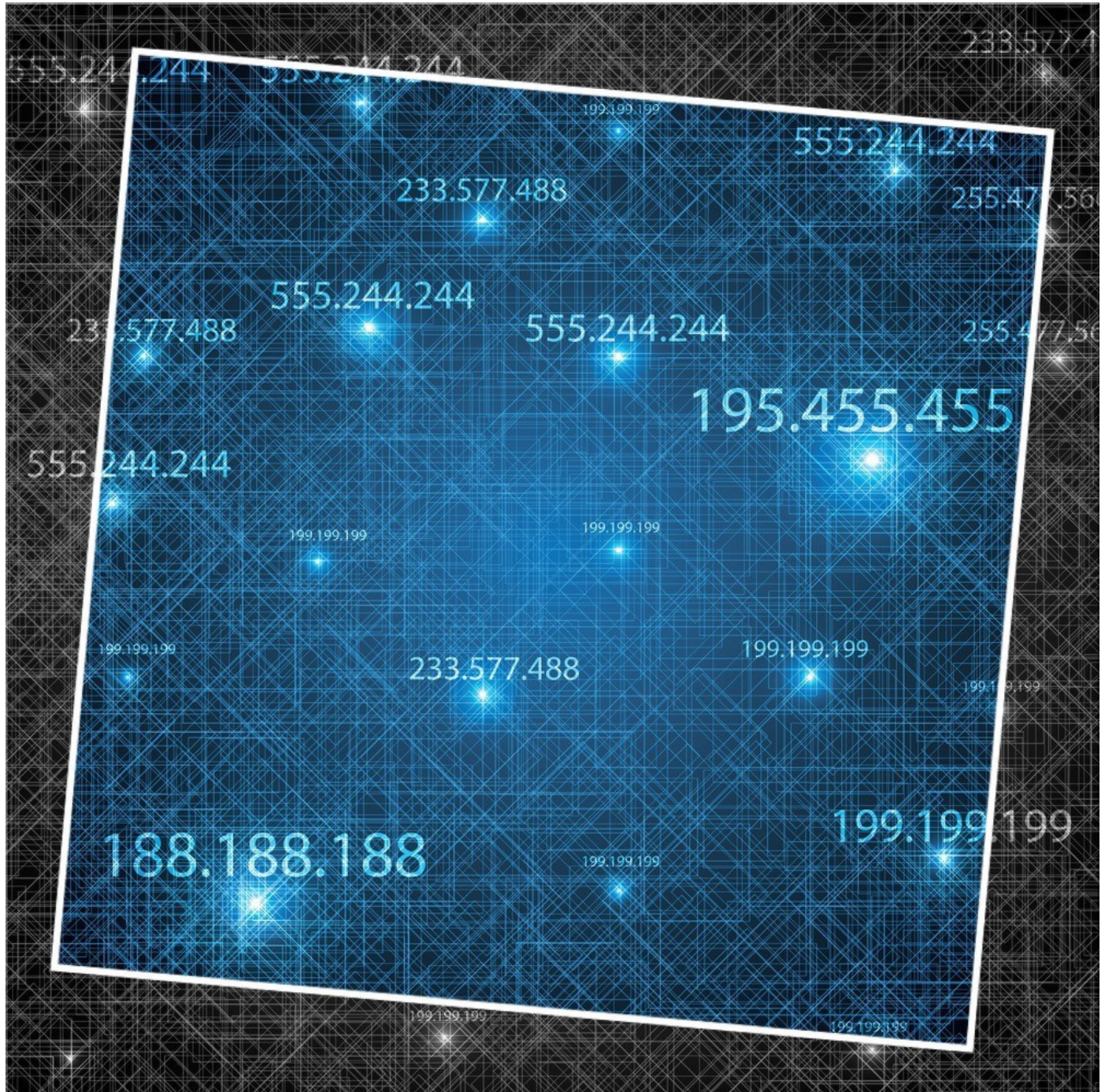
```
PS C:\Users\THM\Downloads> Get-FileHash .\OpenVPN_2.5.1_I601_amd64.msi -Algorithm MD5
Algorithm Hash                                Path
-----
MD5          9D52B46F5DE41B73418F8E0DACEC5E9F  C:\Users\THM\Downloads\OpenVPN_2.5.1_I601_amd64.msi
```

Answer the questions below

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

Conti

### 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](#)):

HTTP Requests		Connections		DNS Requests		Threats	
0		4		4		0	
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:

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

## Task 4 Domain Names (Simple)





















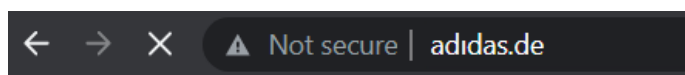
Let's step up the Pyramid of Pain and move on to Domain Names. You can see the transition of colors - from green to teal.

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](#).

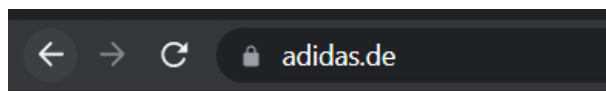
Domain Names can be a little more of a pain for the attacker to change as they would most likely need to purchase the domain, register it and modify DNS records. Unfortunately for defenders, many DNS providers have loose standards and provide APIs to make it even easier for the attacker to change the 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	
	cursorporcelanatoliquido.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 Punycoded attack used by the attackers to redirect users to a malicious domain that seems legitimate at first glance.

What is Punycoded? As per [Wandera](#), "Punycoded 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 `adidas.de` which has the Punycoded 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 Punycoded domain name.

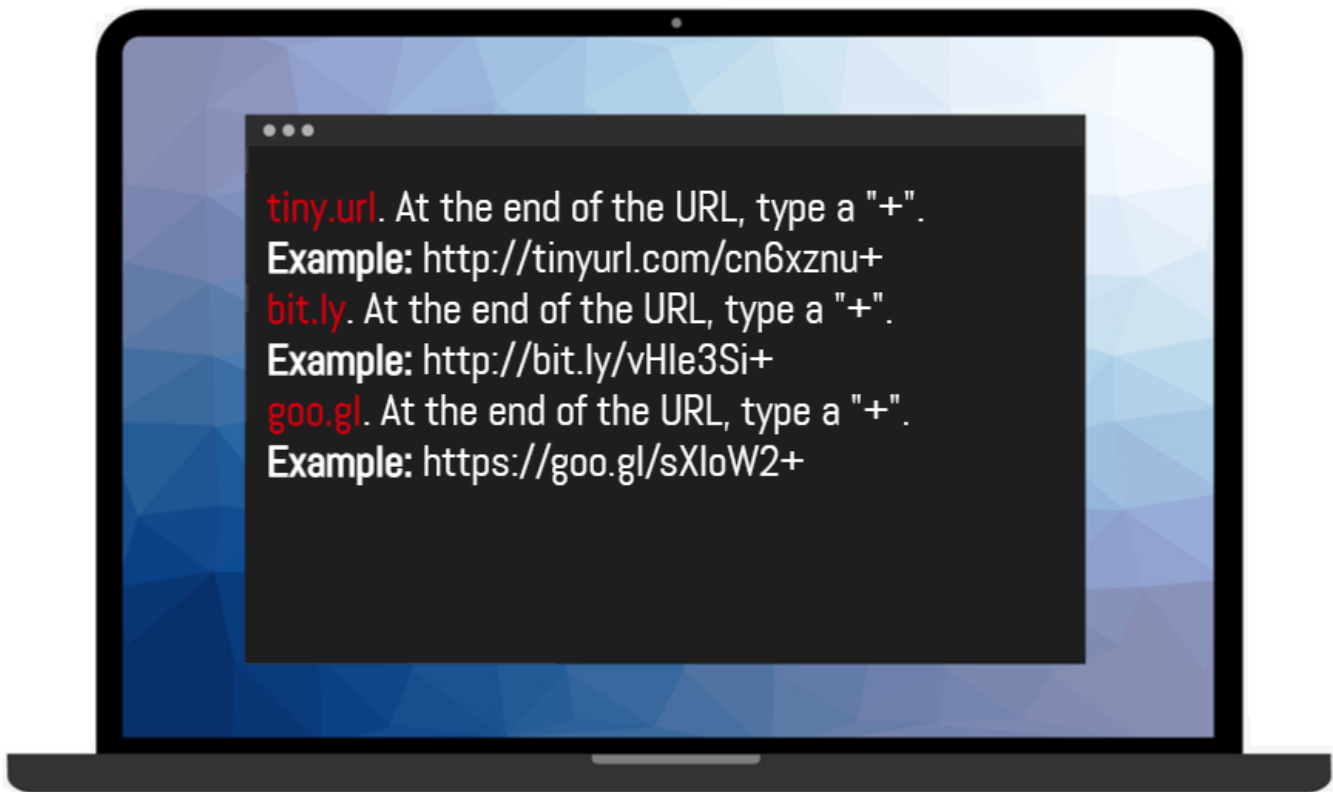
To detect the malicious domains, proxy logs or web server logs can be used.

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.**



Answer the questions below

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`

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

`https://tryhackme.com/`

<https://checktinyurl.com/result?tinyurl=https%3A%2F%2Ftinyurl.com%2Fbw7t8p4u>

## 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:

[illegible]

**The files modified/dropped by the malicious actor:**

+1469ms	C:\Users\admin\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\FIT0N66RBH0VW9F6ARSX.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

Answer the questions below

What is the suspicious IP the victim machine tried to connect to in the screenshot above?

35.214.215.33

Use the tools introduced in task 2 and provide the name of the malware associated with the IP address

emotet

Using your OSINT skills, what is the name of the malicious document associated with the dropped binary?

G\_jugk.exe

Use your OSINT skills and provide the name of the malicious document associated with the dropped binary

CM0-100120 CDW-102220.doc

## Task 6 Network Artifacts (Annoying)



Answer the questions below

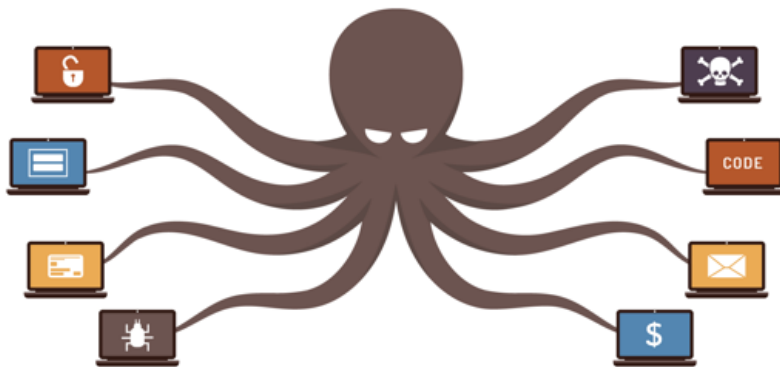
What browser uses the User-Agent string shown in the screenshot above?

Internet Explorer

How many POST requests are in the screenshot from the pcap file?

6

## 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:**

RussianPanda > AppData > Local > Temp				
Organize	Open	Share with	New folder	
<b>Favorites</b>	<b>Name</b>	<b>Date modified</b>	<b>Type</b>	<b>Size</b>
Desktop	s3s8.0	6/20/2021 3:30 PM	0 File	1 KB
Downloads	s3s8.1	6/20/2021 5:36 PM	1 File	1 KB
FLARE	s3s8.2	6/20/2021 5:36 PM	2 File	1 KB
OneDrive	s3s8.3	6/20/2021 5:36 PM	3 File	1 KB
Recent Places	s3s8.4	6/20/2021 5:36 PM	4 File	1 KB
Utilities	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
<b>Libraries</b>	s24s.3	6/20/2021 3:26 PM	3 File	1 KB
Documents	s24s.4	6/20/2021 3:26 PM	4 File	1 KB
Music	Stealer.exe	8/8/2021 6:10 PM	Application	408 KB
Pictures				

**The execution of the suspicious binary:**



 payload.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:

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY 13 +
<b>Basic Properties</b> ⓘ				
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)			

Answer the questions below

Provide the method used to determine similarity between the files

fuzzy hashing

Provide the alternative name for fuzzy hashes without the abbreviation

context triggered piecewise hashes

## 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

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

9

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

## 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

Complete the static site.

## 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.