Threat Hunting Terminology

Module 2

2.1 Threat Hunting Terms

2.2 Threat Hunter Mindset: Threat Intelligence

2.3 Threat Hunter Mindset: Digital Forensics

2.4 Threat Hunting Simulations

Threat Hunting Terms

APT

The first term we'll discuss in this module is **APT,** which stands for **Advanced Persistent Threat.**

This is a word you are probably familiar with, even if you're just getting into threat hunting.

APT

APTs are ***groups*** or ***nation states*** that have a significant amount of resources and infrastructure to conduct their malicious intents.

Their targets range from different industries, government networks, to health care systems to defense systems.

APT

Despite what you might read or see in the headlines, not all APT groups attack US-based networks.

An example of this would be ***Stuxnet***.

APT

Stuxnet was a specific cyberweapon, malware, targeting ***Iran's*** nuclear program.

It was designed to target Siemens Step7 software on computers controlling a PLC (programmable logic controller).

2.1.1 Advanced Persistent Threat

MAP REF

APT

The image on the right is a screenshot of FireEye's Cyber Threat Map. You will see that the US is not the only country targeted. On the contrary, surprisingly, you'll see that the US is attacking another country and the attack signature is labeled as APT.

APT

A couple of things to point out regarding the word **APT**.

Just because a group or nation state is labeled as an APT group it doesn't mean that their techniques are advanced, but they are still considered a persistent threat.

2.1.1 Advanced Persistent Threat

APT

How can they still be considered a persistent threat even though they're not advanced?

One answer. **Resources**.

APT

As mentioned earlier, they could have a significant amount of money, manpower, etc., which will allow them to continually attempt to infiltrate a network for weeks, months, and even years.

APT

Another point to mention is that APT groups are identified various different ways.

One common naming convention is the word **APT** followed by a **number**. Such as **APT 1**.

APT

Below is a small chart displaying some of the different names this particular group, APT 1, might be called.

APT 1	Comment Panda	PLA Unit 61398	TG-8223	Comment Crew

APT

How the APT will be referenced by will depend on which vendor-specific APT report you're reading.

For example, **Mandiant** will refer to ***Comment Crew*** as ***APT 1*** whereas **CrowdStrike** will refer to them as ***Comment Panda***.

2.1.1 Advanced Persistent Threat

MAP REF

APT

APT 1 is a Chinese-based cyber espionage group, a ***nation state***.

It has been discovered that APT 1 is **The 2nd Bureau of the People's Liberation Army General Staff Department's 3rd Department**.

You might see this particular military unit referred to as **The People's Liberation Army (PLA)** or more specifically as **PLA Unit 61398**.

APT

You can read more about this APT group in a report published by Mandiant in 2013 titled "APT1 – Exposing One of China's Cyber Espionage Units".

APT

Florian Roth (@cyb3rops) put together a spreadsheet which lists APT groups and operations.

You can find the spreadsheet here.

TTPs

The next word we'll look at is **TTP**, which stands for ***Tactics, Techniques, and Procedures***.

You might see references to TTPs as ***Tools, Techniques, and Procedures***.

Just make a mental note for when you see the acronym TTP.

TTPs

What are **TTP**s?

This term, as many terms you'll see in cybersecurity, was taken from the military world. In short, **TTP**s represents the methods or signature of the adversary.

TTPs

TTPs tell us the methods the adversary uses to enter the network and how they pivot throughout the network to achieve their goals.

TTPs will help us identify the adversary in future attacks by creating **Indicators of Compromise** (IOCs).

*Click HERE to go back to Slide 66

2.1.2 Tactics, Techniques, & Procedures

MAP REF

TTPs

IOCs

IOCs are artifacts that were gathered from an active intrusion or previous intrusion that are used to identify a particular adversary.

It will range from MD5 hashes, IP addresses, names of EXEs used, etc.

2.1.2 Tactics, Techniques, & Procedures

MAP REF

TTPs

IOCs

For example, we'll look APT 1 & list certain IOCs for APT 1.

2.1.2 Tactics, Techniques, & Procedures

MAP REF

TTPs

IOCs

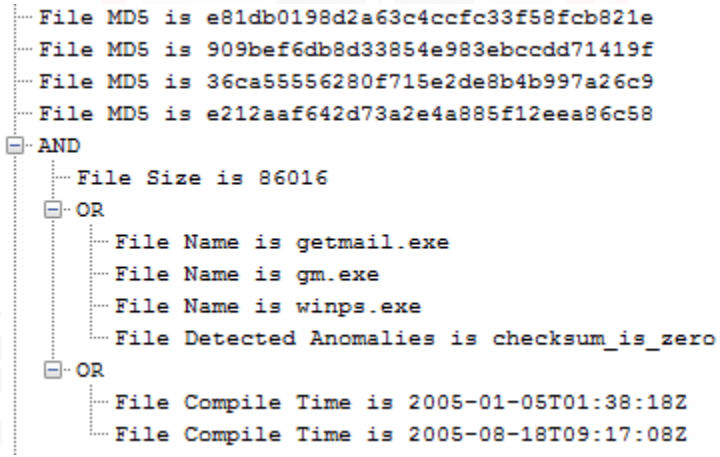
APT 1 uses two custom utilities to steal emails from their victims:

- GETMAIL: malware used to extract email messages and attachments from Outlook PST files.
- MAPIGET: malware used to extract email messages and attachments from an Exchange server.

TTPs

IOCs

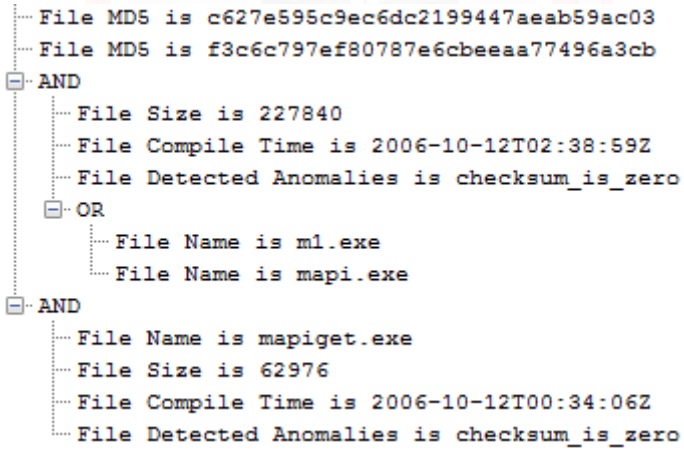
Below is a snippet of the IOC for GETMAIL.



TTPs

IOCs

This is a snippet of the IOC for MAPIGET.



2.1.2 Tactics, Techniques, & Procedures

MAP REF

TTPs

IOCs

We'll discuss IOCs and various IOC-based tools in later modules.

Pyramid of Pain

We'll now look at the **Pyramid of Pain** which:

- Is a visual that will layer the potential usefulness of indicators that will aide you on detecting an adversary.
- Measures how difficult it will be to obtain that particular indicator or indicators, as well as the impact on obtaining the intel on them.

Pyramid of Pain

The Pyramid of Pain was created by David Bianco (FireEye) and he discusses the Pyramid of Pain in a presentation titled ***Intel-Driven Detection and Response to Increase Your Adversary's Cost of Operations***.

*Click HERE to go back to Slide 43
*Click HERE to go back to Slide 47

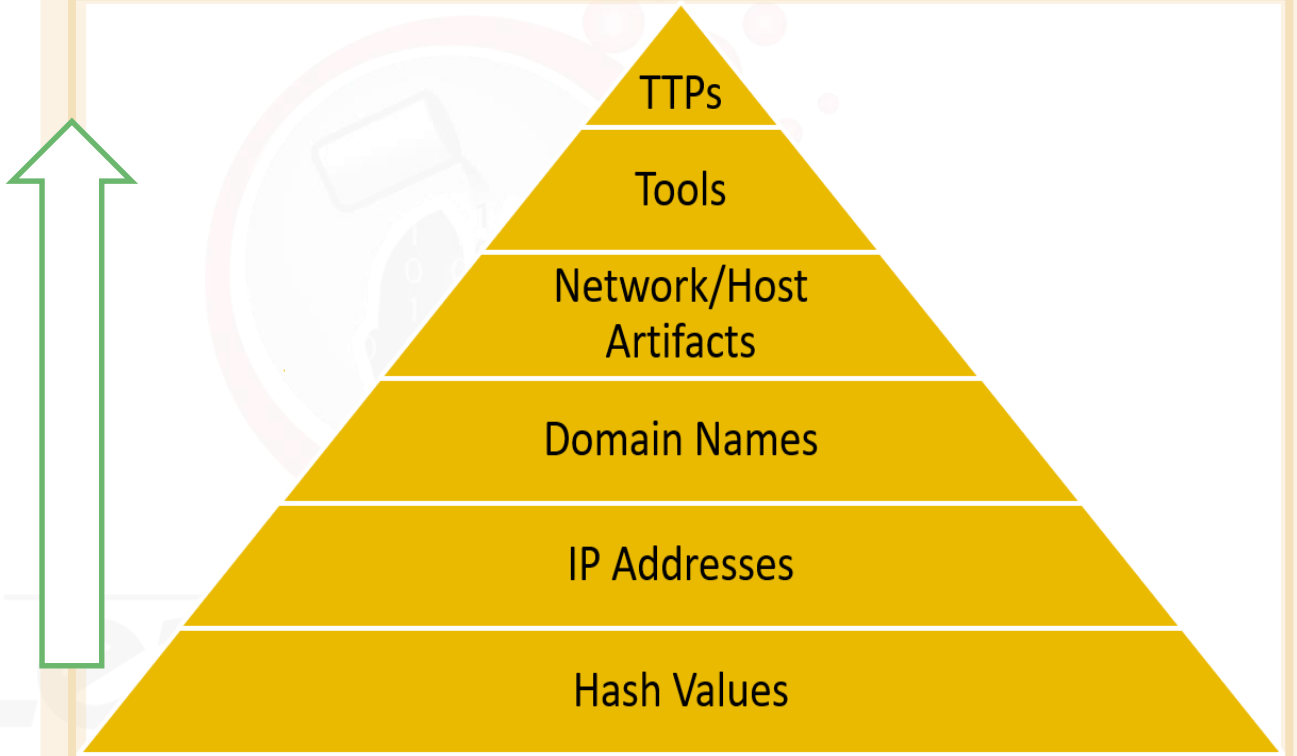
Pyramid of Pain

The following slides will outline the Pyramid of Pain and detail each layer of the Pyramid of Pain.

2.1.3 Pyramid of Pain

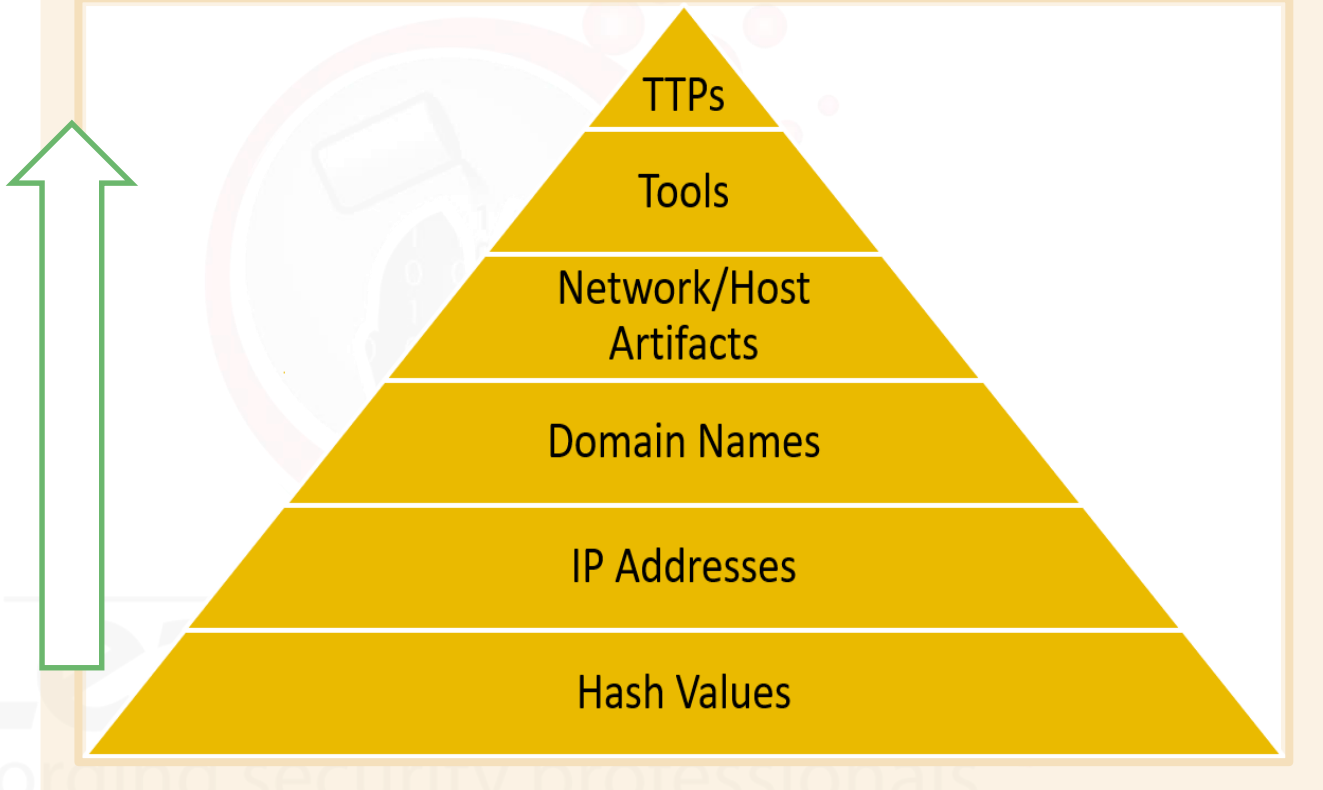
Pyramid of Pain

As we go up the Pyramid of Pain the harder it will be to obtain the adversary-specific IOCs.



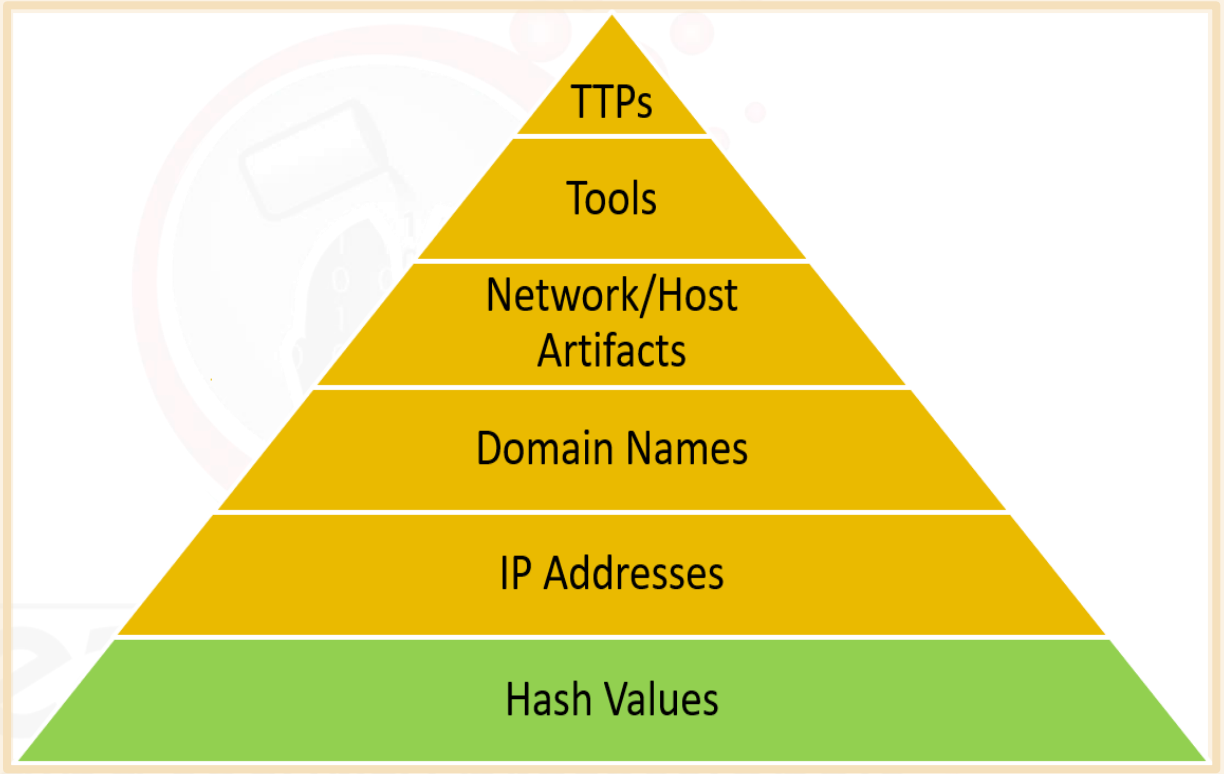
Pyramid of Pain

On the flip side, if we obtain those adversary-specific IOCs then we're forcing the adversary to change their attack methods, which is not an easy task for them.



Pyramid of Pain

Let's look at Hash Values.



Pyramid of Pain

Hash values

1. Hash Values:

- Hash values are good but the least reliable, compared to other indicators.
- The reason hash values are the least reliable is because they're easy to change.

Pyramid of Pain

Hash values

What is a **hash value**?

From Microsoft, “A hash value is a numeric value of a fixed length that uniquely identifies data”. We use these numeric values as signatures.

Pyramid of Pain

Hash values

You might have seen this when you download a binary (EXE). The developer will display the hash value of the binary. You use the hash value of the binary that was downloaded and compare it to the value on the developer's site. This will confirm that that binary you downloaded has not been tampered with and it's authenticity.

Pyramid of Pain

Hash values

The following snippet is from the Putty download page.

Checksum files

Cryptographic checksums for all the above files

MD5:	md5sums	(or by FTP)	(signature)
SHA-1:	sha1sums	(or by FTP)	(signature)
SHA-256:	sha256sums	(or by FTP)	(signature)
SHA-512:	sha512sums	(or by FTP)	(signature)

Pyramid of Pain

Hash values

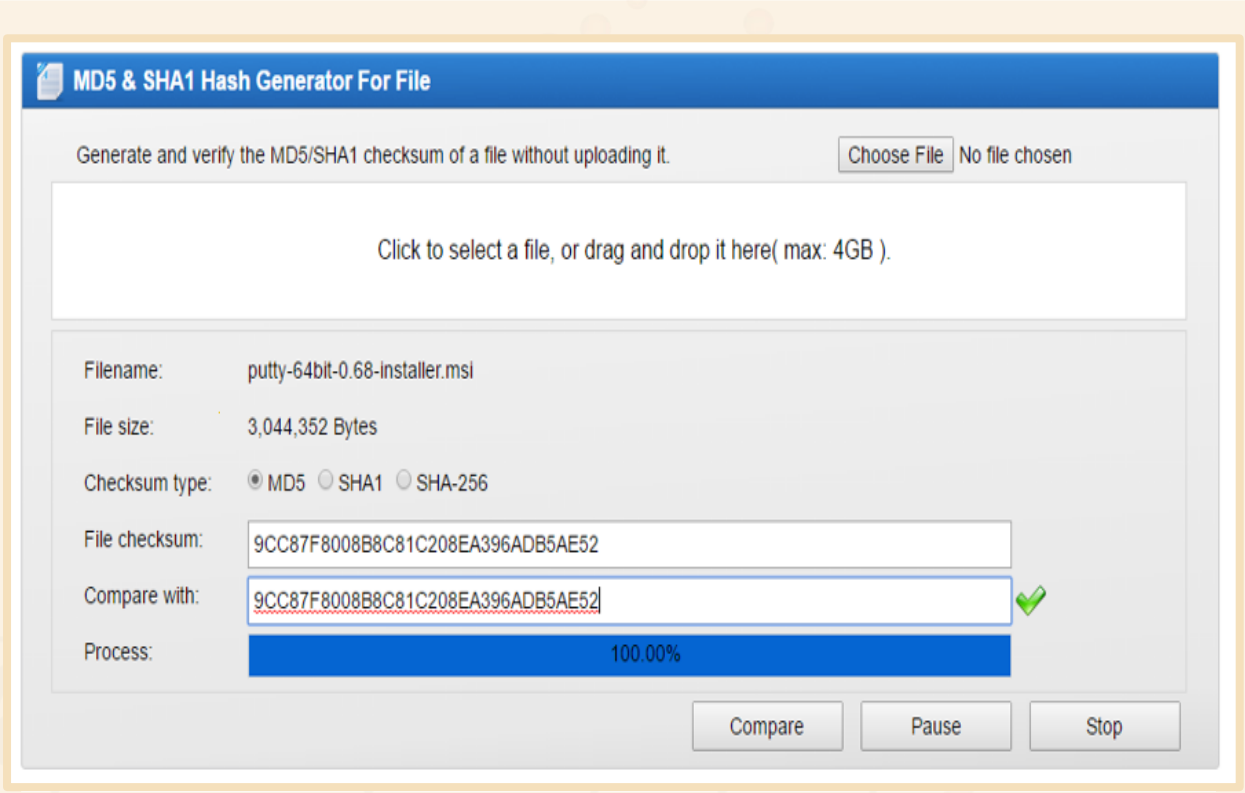
Below is a list of MD5 values.

```
1c31b9d59c33124cf19aafe5ca4d8d77  w64/plink.exe
9206dae8b89a9e366b88f57a117068ea  w64/pageant.exe
be183d872773a130efb8bf1f1c60b6db  w64/puttytel.exe
caba0287018a2f1c0f4e7ba357f9072d  w64/puttygen.exe
5ca0a9e56499c658d2790be7113930f1  w64/putty.zip
8ca5e64d33ff45f0278de27aa4994434  w64/pscp.exe
9cc87f8008b8c81c208ea396adb5ae52  w64/putty-64bit-0.68-installer.msi
a04e72503528dfc132c48e95fa3160ad  w64/putty.exe
fc10492df39f9be3d8c139e2828a59da  w64/psftp.exe
```

Pyramid of Pain

Hash values

The screenshot on the right verifies the MSI that was downloaded is authentic based on checksum (MD5) listed on the download page.



Pyramid of Pain

Hash values

Why are MD5 hashes unreliable?

If you use it as the sole identifier for a binary, with no other IOCs, that MD5 value can change by a slight modification to the source code or by recompiling the source code with a different compiler.

Pyramid of Pain

Hash values

If your IOC just became useless, it’s easy to change and has no real impact on the adversary.

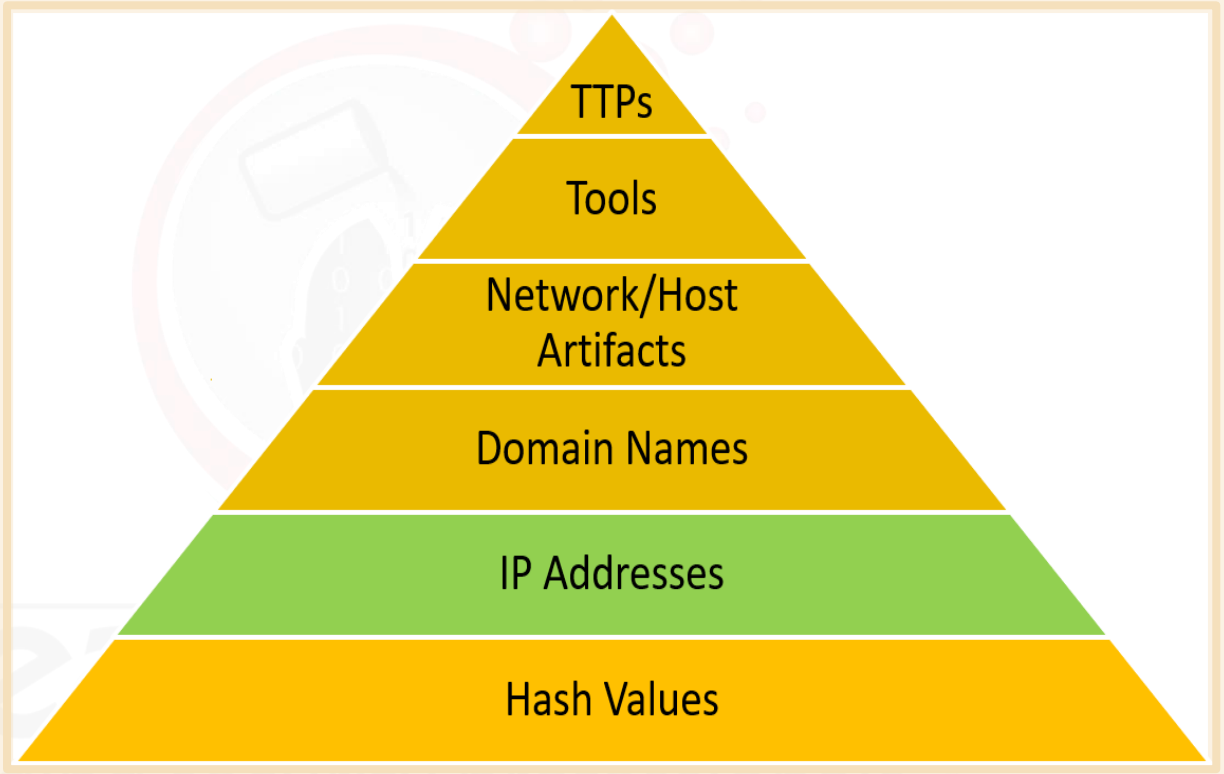
2.1.3 Pyramid of Pain

MAP REF

Pyramid of Pain

IP Addresses

Let's look at IP Addresses.



Pyramid of Pain

IP Addresses

2. IP Addresses:

- The probability that an adversary is using some sort of anonymity channel to mask their actual IP address is high.
  - By anonymity we are referring to a proxy, VPN, or TOR for example.
- IP addresses are easy to change.

Pyramid of Pain

IP Addresses

Below is a snippet from the presentation mentioned in slide 28 with examples of IP addresses.

Dotted Decimal 192.168.1.1 **Dotted Hex** 0xC0.0xA8.0x01.0x01 **Dotted Octal** 0300.0250.0001.0001	**Decimal** 3232235777 **Hex** 0xC0A80101 **Octal** 030052000401

Pyramid of Pain

IP Addresses

If the IP Addresses are hardcoded then these IPs can be blacklisted and prevented to communicate outbound.

This will give some work to the adversary because now the tools and scripts have to point to a new IP or IP addresses.

Again, this is the case if IP Addresses are **hardcoded**.

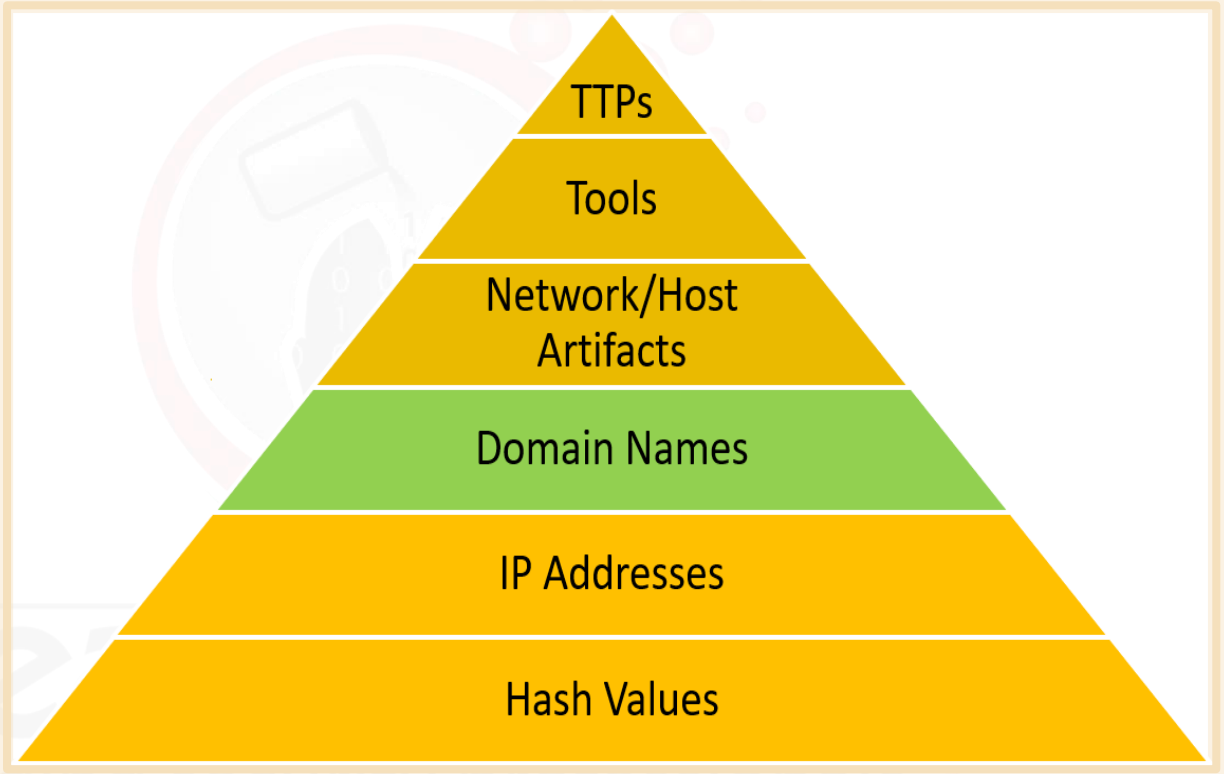
2.1.3 Pyramid of Pain

MAP REF

Pyramid of Pain

Domain names

Let’s look at Domain names.



Pyramid of Pain

Domain names

3. Domain Names:

- Dynamic DNS providers help the updating process with APIs.
- Easy to change.

Pyramid of Pain

Domain names

Below is a snippet from the presentation mentioned in slide 28 with examples of domain names.

Unicode 邪悪なドメイン.com	**Legitimate Domain** rvasec.com
Punycode Xn—q9j5f9d1dzdq306auhtd.com	**Malicious Homograph** rvasec.com

*Click HERE to go back to Slide 52

Pyramid of Pain

Domain names

In the chart illustrated in the previous slide we can see that a domain name can be displayed or accessed in various fashions.

Pyramid of Pain

Domain names

We will not discuss every type of format a domain name can be displayed as or accessed by.

Instead we'll discuss the lesser known techniques to display a domain name.

Pyramid of Pain

Domain names

What is punycode?

From punycoder.com, **Punycode** is a special encoding used to convert Unicode characters to ASCII. Punycode is used to encode ***IDN***s (Internationalized Domain Names).

Pyramid of Pain

Domain names

Below is an example of text in Unicode and converted to Punycode.

Text	Punycode
Example: 點看	Example: xn--c1yn36f

Pyramid of Pain

Domain names

Next we'll look at **IDN Homograph Attacks**.

In the snippet seen in slide 47, it's called a Malicious Homograph.

Pyramid of Pain

Domain names

In the same slide, the domain listed under Legitimate Domain and Malicious Homograph look identical but in fact they are different.

Legitimate Domain
rvasec.com

Malicious Homograph
rvasec.com

Pyramid of Pain

Domain names

In an IDN Homograph Attack malicious threat actors will exploit the fact that many different characters look alike.

This is similar to another phrase known as **typo squatting**.

Pyramid of Pain

Domain names

Please reference the following Black Hat presentation titled "Unraveling Unicode: A Bag of Tricks for Bug Hunting" for more information and additional references on the subject.

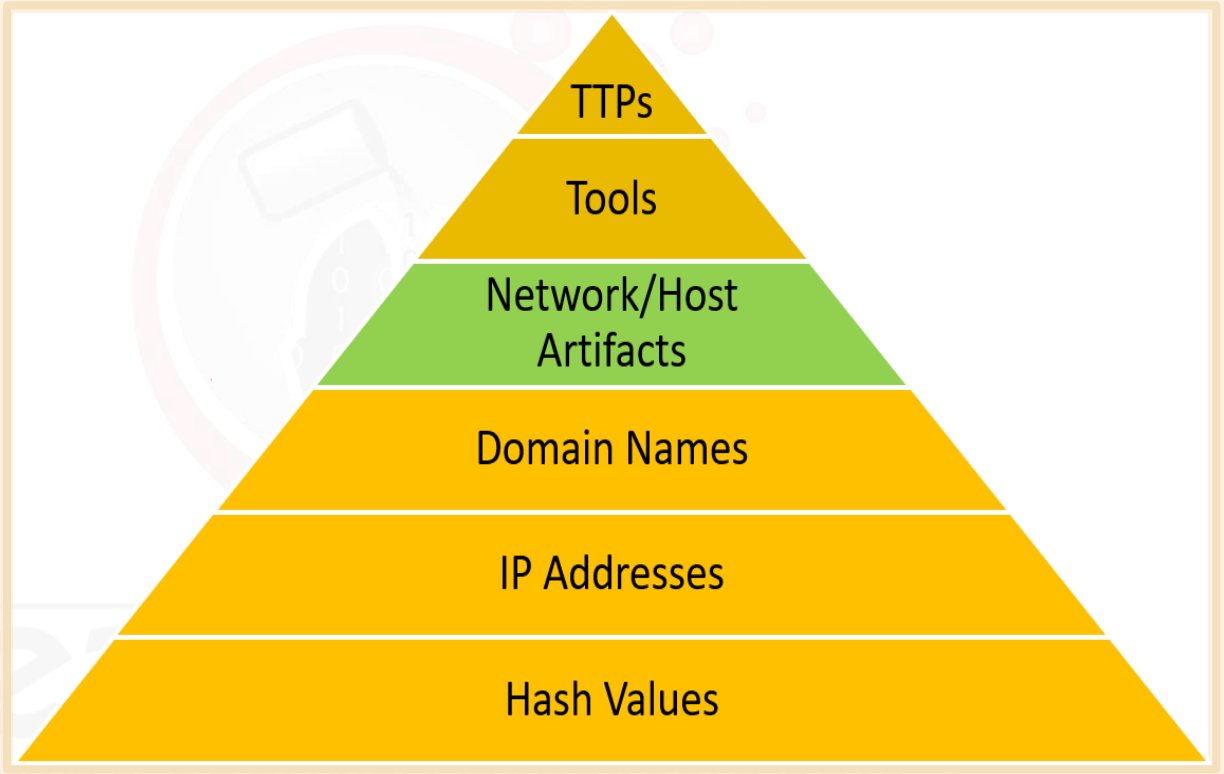
2.1.3 Pyramid of Pain

MAP REF

Pyramid of Pain

Network/Host Artifacts

Let's look at Network/Host Artifacts.



Pyramid of Pain

Network/Host Artifacts

4. Network & Host Artifacts

- Clues the adversary left for us within network packets and in the endpoint systems.

Pyramid of Pain

Network/Host Artifacts

An example of a Network Artifact and a Host Artifact shown below:

Network Artifacts	Host Artifacts
Rare User-Agent strings	Specific Registry key
Traffic on non-traditional ports (i.e. 6667)	Process connected on port 80 that is not a browser

Pyramid of Pain

Network/Host Artifacts

This is an example of a network artifact, a fake user-agent.

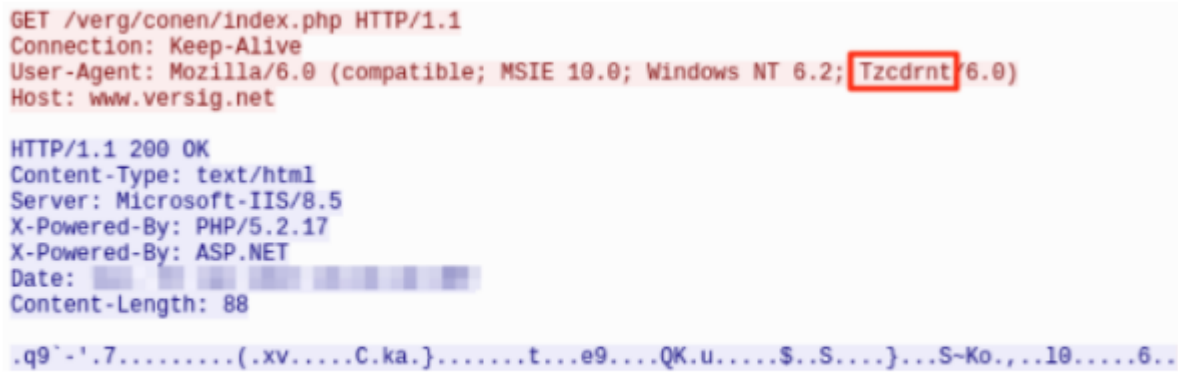


Figure 9: ZeroT initial beacon over HTTP requesting URL configuration

Credit: https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

Pyramid of Pain

Network/Host Artifacts

The next 2 slides will list what will really hurt an adversary if we get really good at detecting them.

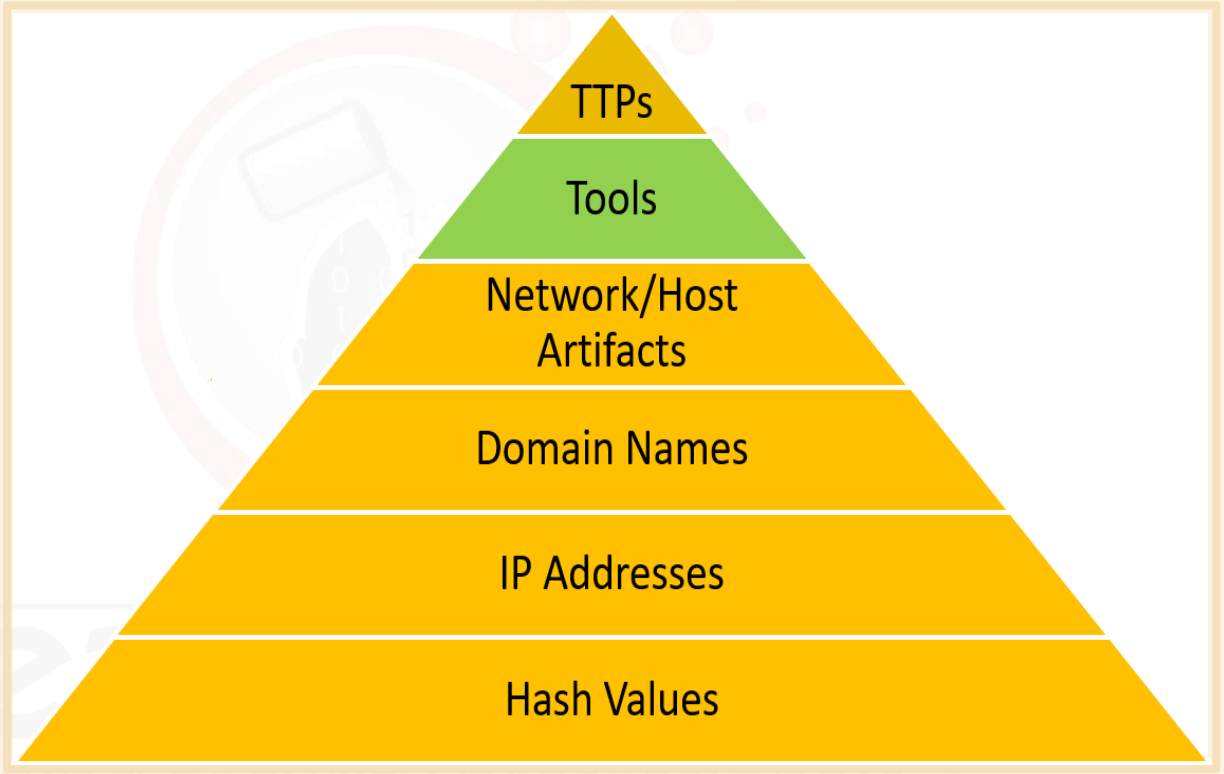
2.1.3 Pyramid of Pain

MAP REF

Pyramid of Pain

Tools

Let’s look at Tools.



Pyramid of Pain

Tools

5. Tools:

- An APT group will most likely stick to a consistent set of tools.

Pyramid of Pain

Tools

If you're an experienced penetration tester, then you know this to be true. You won't just grab a tool you won't normally use if you're conducting an SQL attack. You will use your tool of preference, such as SQLMap or similar tool.

Pyramid of Pain

Tools

If you get good at detecting a particular tool, this will force the adversary to use a new tool because the tool they currently use won't work against you anymore.

This will lead to more work on behalf of the adversary. However, this could lead to the adversary bypassing your network.

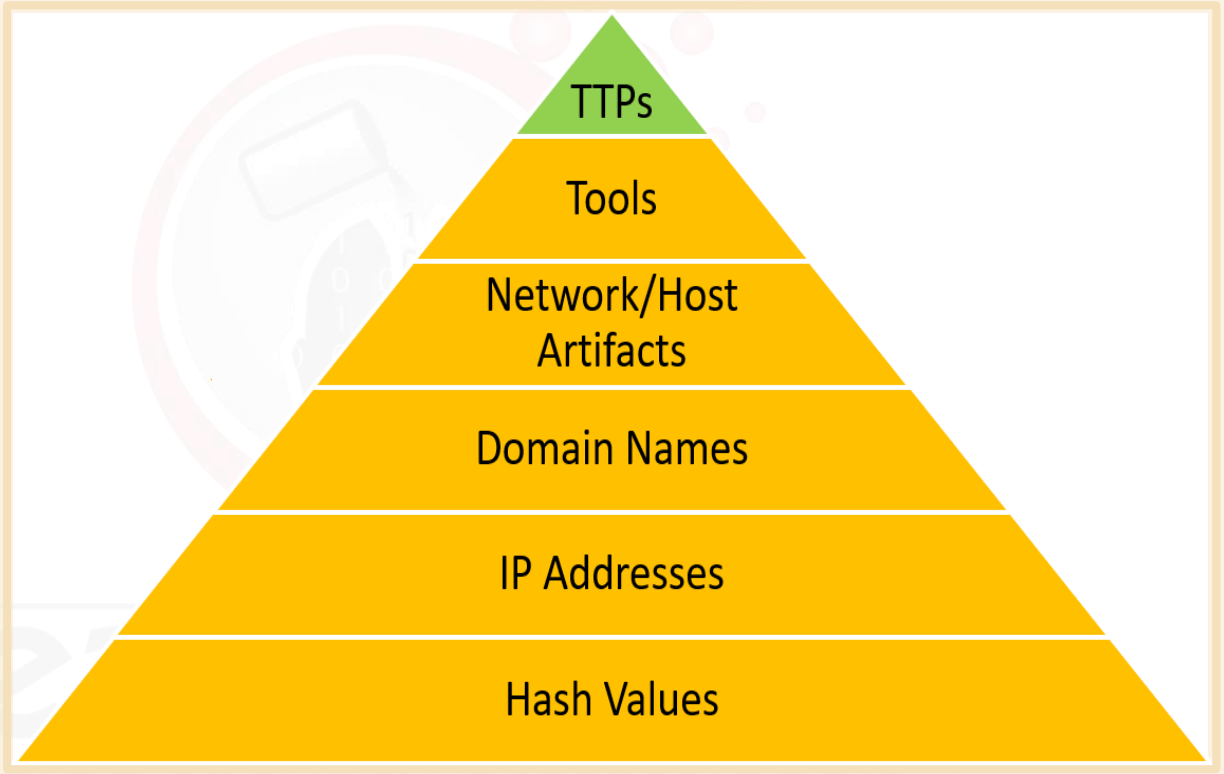
2.1.3 Pyramid of Pain

MAP REF

Pyramid of Pain

TTPs

Lastly, let's look at TTPs.



Pyramid of Pain

TTPs

6. TTPs:

- Remember in slide 20, TTPs represents the methods or signatures of the adversary.

- In David Bianco's presentation, "Pyramid of Pain: Intel-Driven Detection and Response to Increase Your Adversary's Cost of Operations", he defines TTPs as the **expression of the attacker's training**.

Pyramid of Pain

TTPs

Retraining is hard and expensive.

Imagine re-training 1,000 operators so that the current TTPs and IOCs gathered on them no longer prove to be fruitful and new intel has to be gathered. That task is easier said than done but if they have the funding, it is not impossible.

Cyber Kill Chain

Let's now discuss the **Cyber Kill Chain**.

This term also stems from the military. The military term is kill chain. Kill chain in both cases refers to the different stages of an attack.

2.1.4 Cyber Kill Chain Model

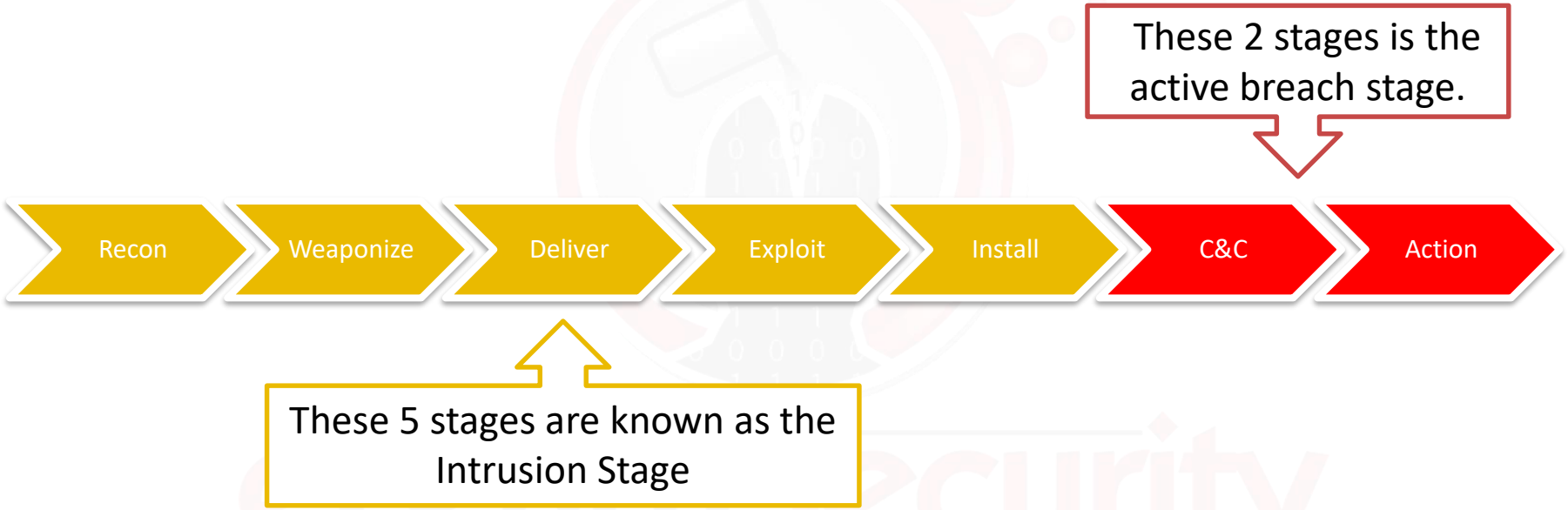
Cyber Kill Chain

Lockheed Martin is credited for applying this term to information security.

2.1.4 Cyber Kill Chain Model

MAP REF

Cyber Kill Chain



2.1.4 Cyber Kill Chain Model

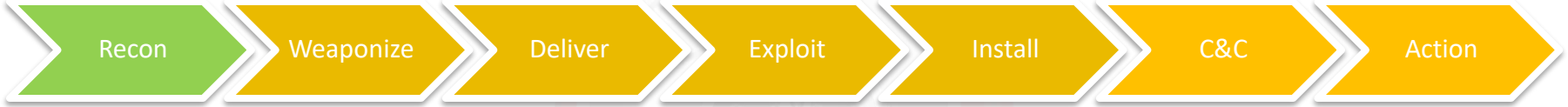
Cyber Kill Chain

Let’s see an example of the Cyber Kill Chain Model through a sample attack scenario.

2.1.4 Cyber Kill Chain Model

MAP REF

Cyber Kill Chain

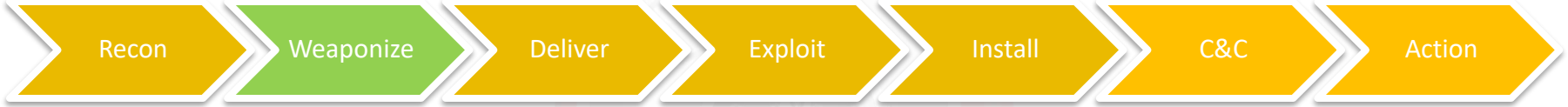


Recon: This step involves passive scanning plus OSINT (i.e. social media, search engines, etc). It can also involve active scanning public-facing IPs.

2.1.4 Cyber Kill Chain Model

MAP REF

Cyber Kill Chain

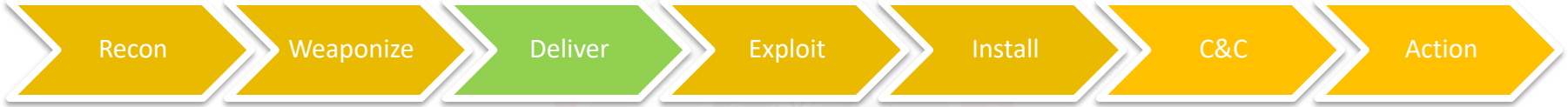


Weaponize: This is where the RAT (Remote Access Tool) is added to the exploit. The exploit can reside on a web page or a malicious macro-based document attached to an email. In this stage the adversary also considers the method of delivery.

2.1.4 Cyber Kill Chain Model

MAP REF

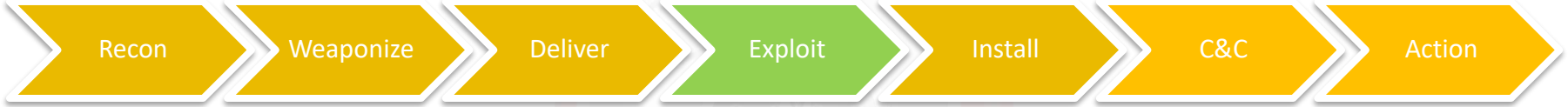
Cyber Kill Chain



Deliver: This phase covers the delivery of the weaponized tool. The delivery method can be via email, via social media, or a watering hole attack, to name a few.

2.1.4 Cyber Kill Chain Model

Cyber Kill Chain

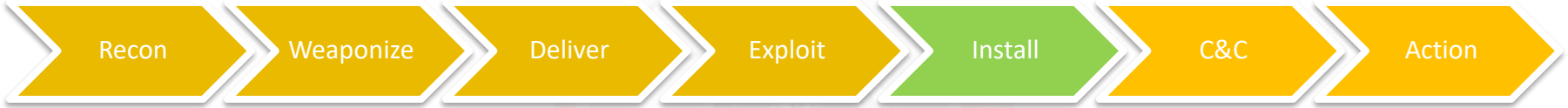


Exploit: This phase is the actual exploitation. This is when a user opens the document attached to an email, clicks a link, etc. This can be a 2-step process where a loader is used to download the actual RAT. The loader will typically be small in size and reside only in memory.

2.1.4 Cyber Kill Chain Model

MAP REF

Cyber Kill Chain

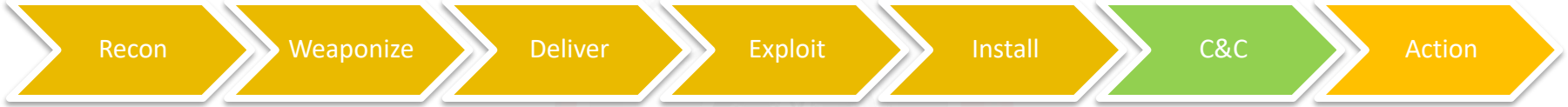


Install: At this point, in most cases, additional tools are installed via the RAT. Other tools can be a network scanner, a keylogger, etc.

2.1.4 Cyber Kill Chain Model

MAP REF

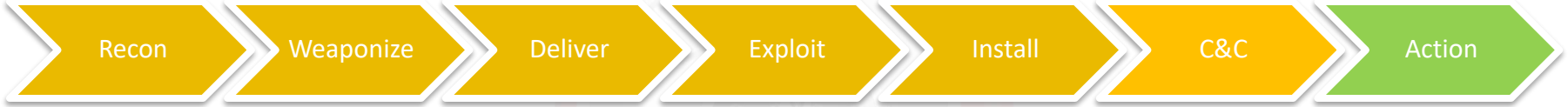
Cyber Kill Chain



C&C: This is the command & control (C2) phase. This is when the victim's machine will call out to an IP or domain and provide the adversary command-line access to the box.

2.1.4 Cyber Kill Chain Model

Cyber Kill Chain



Action: This is where the goal is achieved. The goal can be exfiltration. This is when:

- the adversary scans the network, looks/reviews data, and grabs what they are looking for.
- what you're protecting leaves the network.

GAME OVER!

Cyber Kill Chain

2 things to remember about the Cyber Kill Chain:

It's a cyclical process. It's not linear.

1. What that means is that once an adversary gets a foothold on a box (machine), they will not stay there. They will begin from the start of the kill chain. They will perform internal recon and look for other machines to exploit. They will also look to cover their tracks. Most likely the box they'll establish the C2 channel with, will not be the initial box they exploited.

2. Our goal as defenders is to stop the adversary from progressing up the kill chain and stopping them. Doing this in one of the ***early stages*** of the chain is always preferred.

Cyber Kill Chain

Other companies such as FireEye and Mitre have developed their own model for the Cyber Kill Chain. You will see references to these models as "**Attack Lifecycle**".

You can read up more on their attack models by doing a quick search online to learn more about them.

Diamond Model

The last model we'll look at is called the **Diamond Model**. The paper describing the Diamond Model was released in 2013 by ***The Center for Cyber Intelligence Analysis and Threat Research***.

The link to official paper is here.

Diamond Model

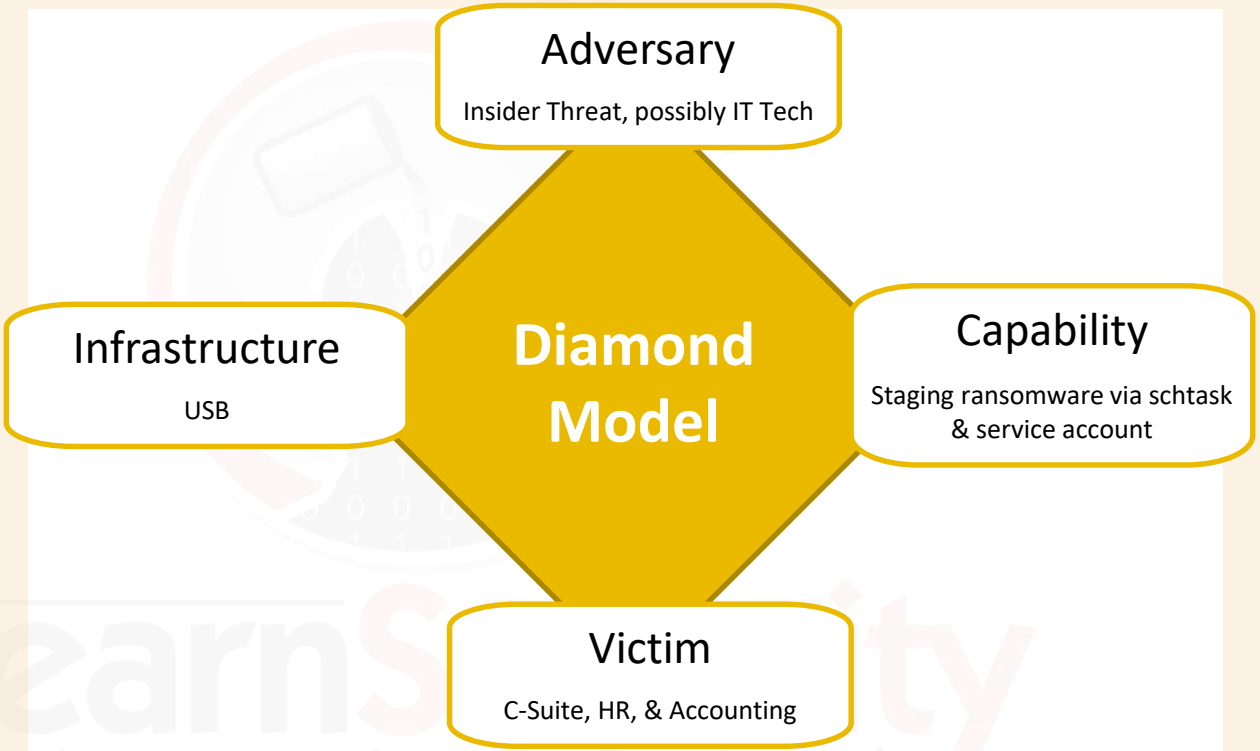
What is the Diamond Model?

”In its simplest form, the model describes that an ***adversary*** deploys a ***capability*** over some ***infrastructure*** against a ***victim***.”*

** The Center for Cyber Intelligence Analysis and Threat Research.*

Diamond Model

Here is a visual depiction of the Diamond Model.



Diamond Model

In the same paper referenced on Slide 81, under Diamond Event, Axiom 1, it states:

“For every intrusion event there exists an adversary taking a step towards an intended goal by using a capability over infrastructure against a victim to produce a result.”

Diamond Model

The Diamond Model can be used in conjunction with the Cyber Kill Chain model.

Remember the goal is to prevent the adversary from reaching his/her goal.

Diamond Model

Axiom 4, it states:

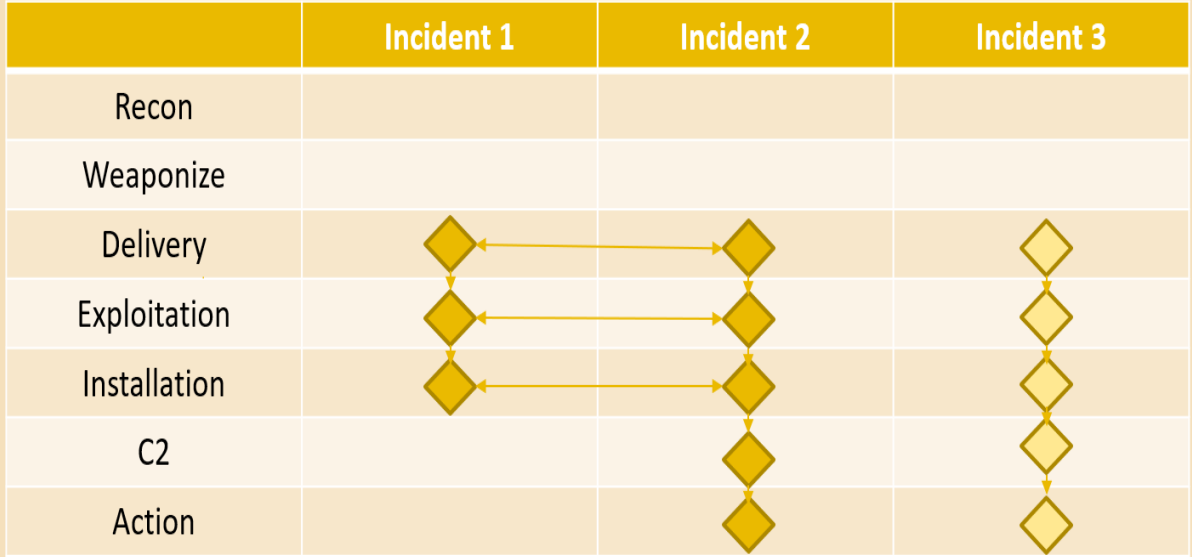
"Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result."

2.1.5 The Diamond Model

Diamond Model

The image on the right illustrates the conjunction between the Cyber Kill Chain and the Diamond Model.

The simple example, illustrates information gathered from 3 incidents. Each labeled as Incident 1, Incident 2, & Incident 3.



Diamond Model

Each stage of the Kill Chain the Diamond Model is used to collect data on the attack.

In Incident 2, based on similarities of Incident 1, the hypothesis would be that it's the same adversary.

Diamond Model

Incident 3 shows no correlation between Incident 1 or 2 so its led to believe that it's a different adversary.

Now you have information where if these 2 adversaries strike again, you have create indicators that will assist you on stopping them.

Diamond Model

Remember to find a methodology and model that works for you. Everything within cybersecurity should follow some methodology.

Threat Hunting Mindset: Threat Intelligence

In most cases, a threat hunter has one of two mindsets.

One hunter will rely mostly on **threat intelligence** while the other will rely mostly on **digital forensics**.

Threat Intel

Let’s talk about threat intelligence first.

What is threat intelligence?

Threat Intel

A simple definition of **Threat Intelligence** is data on threats. The information will come in various forms and the information could be obtained through various channels such as open source, social media, etc.

Threat Intel

The data can be IP addresses, netblocks, domains, MD5 hashes, etc. The threats can be APTs, cyber crime groups, hacktivists, etc.

Threat Intel

Data is exactly that, just data. For the information to become intelligence, it has to be analyzed. Once it's analyzed and it becomes actionable then it's categorized as intelligence because there is context around the information. Some data might not be applicable to your organization.

Threat Intel

An appliance will be used to sift through all that data so you can focus on what needs to be focused on.

Threat Intel

It’s also important to mention that Threat Intelligence can be divided into 3 types:

1. Strategic: Who, Why, & Where
2. Tactical: What & When
3. Operational: How

Threat Intel

As hunters, we're probably more focused on tactical and operational intelligence; how the adversary does what they do, so we can detect it and prevent further escalation through the attack chain.

The 3 Types of Threat Intelligence

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

In slide 104, we outlined 3 types of Threat Intelligence. In this section we'll look at each type briefly.

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

1. Strategic: Who, Why, & Where
2. Tactical: What & When
3. Operational: How

Threat Intel

Strategic

Strategic Intelligence is designed to assist senior management to make informed decisions about the security budget and security strategies (such as risk management).

With specific intelligence, senior management ***might*** obtain answers to the following questions.

Threat Intel

Strategic

Who is the adversary?

Why are they targeting you?

Where have they attacked prior to attacking you?

Note: Sometimes it's not easy to provide answers to those questions.

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

1. Strategic: Who, Why, & Where
2. Tactical: What & When
3. Operational: How

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

Tactical

Tactical Intelligence, which merges into Operational Intelligence, deals with the adversary's TTPs. This is where the Cyber Kill Chain and Diamond Models are used to attempt to identify the adversary's pattern of attacks, their signature.

Threat Intel

Tactical

As stated earlier, Tactical Intelligence addresses the what and when.

What is the adversary's toolset?

When are these attacks orchestrated?

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

1. Strategic: Who, Why, & Where
2. Tactical: What & When
3. Operational: How

Threat Intel

Operational

Operational Intelligence deals with the actual indicators, the IOCs, and it addresses the how.

How is the adversary conducting their attack?

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

Operational

Remember that Operational Intelligence can merge into Tactical Intelligence.

In most cases, you will see it plainly identified as Operational Intelligence.

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

Operational

ISACs is one of several avenues to assist with obtaining this subset of intelligence. **ISACs** are ***Information Sharing and Analysis Centers***.

We will look into this further in the next module.

2.2.2 The 3 Types of Threat Intelligence

Threat Intel

In summary, this type of hunter will be focused on ***known*** information, data that will assist him/her in the hunt.

Threat Hunting Mindset: Digital Forensics

Digital Forensics

Now we'll look at the other type of hunter.

This hunter will primarily lean on digital forensics in his/her hunt, hunting for the ***unknown***.

Digital Forensics

Now they will still use threat intelligence, it would be foolish not to, but this type of hunter will not solely rely on that.

This hunter will take it a step further and analyze digital artifacts to see if there is any indication of a threat.

Digital Forensics

This hunter doesn't wait for an alert from one of the appliances regarding a potential threat. This hunter is actually hunting.

The phrase '**threat hunter**' says it all.

Someone just looking & analyzing data would be considered an analyst.

The hunter is proactively hunting!

Digital Forensics

This type of hunter will be looking at network traffic.

They will attempt to spot anything out of the ordinary, such as malicious traffic masquerading as legitimate traffic.

Digital Forensics

This type of hunter will conduct memory analysis and inspect running processes to see if anything suspicious is running.

For example, a process running on port 80 or 443 that is not a browser.

Digital Forensics

This type of hunter might also reverse engineer binaries to see if the binary is legitimate or malicious.

Not all hunters have this ability, but in smaller organizations where a hunter is expected to wear more than one hat, this might be the case.

Digital Forensics

The goal of this course is to give you a mindset of a hunter that can analyze threat data but also take it a step further and hunt for the unknown.

Threat Hunting Simulations

Threat Hunting is a very wide topic that requires multiple skills that you can acquire in separate courses. The goal of this course is to provide you with mindset, methodologies and practical skills to perform a hunt.

One point we felt that shouldn’t be overlooked is **Threat Hunting Simulations**.

The concept behind this is for the hunter to always practice and train, so that they are able to hunt effectively.

Think about soldiers.

Once they pass boot camp and are trained they don't end training forever.

They are constantly training to ensure their skills don't get rusty and that they don't forget their training.

This also includes law enforcement personnel as well.

We feel that a hunter should occasionally participate in a war game type of environment.

Penetration Testers exercise this practice as well. They're called Capture the Flag activities.

These platforms are used as competition, but some are use to train and enhance ones skill.

In summary, the threat landscape is constantly evolving. As hunters we have to stay current and not get rusty at hunting.

This concludes this module on Threat Hunting.

We have covered:

- ✓ Various terms associated with Threat Hunting
- ✓ Various attack models and methodologies
- ✓ The two threat hunter mindsets: intel and forensics
- ✓ The importance of continual training

References

References

FireEye Threat Map

Mandiant APT 1 Report

APT Groups & Operations

Pyramid of Pain

Unraveling Unicode

Cyber Kill Chain

Diamond Model