MODULE 01 | INTRODUCTION TO THREAT HUNTING

By: Mohamed Adel (m0_4de1)

Gmail: mohamed.adel76765@gmail.com

Introduction

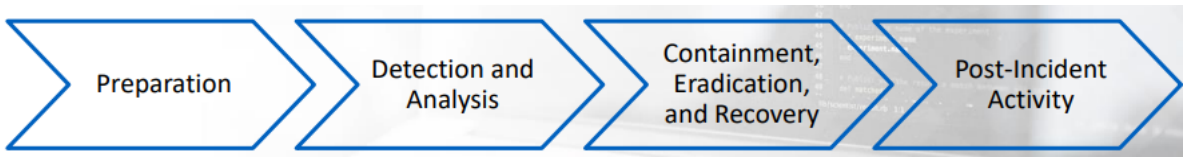
- Cybercriminals are constantly evolving and becoming better at bypassing traditional defenses. While they help, they don't completely prevent a skilled intruder from entering your network. Automated detection tools alone are not enough to detect advanced, stealthy attacks.
- Threat hunting is the human-centric process of proactively searching data and discovering cyber threats. It is a drastic change from the traditional reactive approach of waiting for an internal system, such as an IDS, or law enforcement, to notify them that they have been breached. The hunter detects threats that nothing else detected.
- Threat hunting aims to reduce the dwell time by identifying threats in a very early stage of the infection. By doing so, it may be possible to prevent attackers from gaining a stronger foothold in the environment and remove them from the network.
- Threat Intelligence is often utilized during the hunt to develop techniques and carry out necessary actions to protect systems from compromise.

Hunting:

- Is an offensive-based strategy
- Requires the hunter to think like an attacker
- Requires strong practical understanding of cyber threats and the cyber-kill chain
- Requires you to know your environment
- Is easier with quality data and resource

Incident Response

- Let’s briefly go over each phase of the incident response process defined by NIST.



Preparation phase

- Outlining everyone’s responsibilities, hardware, tools, documentation, etc.
- Taking steps to reduce the probability of an incident from ever occurring

Detection and Analysis phase

- The IR team would confirm if a breach took place.
- They would analyze all the symptoms which were reported and confirm if the situation would be classified as an incident.

Containment, Eradication, and Recovery phase

- The IR team would gather intel and create signatures that will aid them in identifying each compromised system. With this information, countermeasures can be put in place to neutralize the attacker and attempt to restore systems/data back to normal.

Post-Incident Activity

- In this phase, the goal is to improve the overall security posture of the organization and to assure that a similar incident will not happen again.

How does threat hunting correlate to the phases of IR?

- **Preparation phase:** A threat hunter or team can’t operate without rules of engagement.

They need predefined terms on how to operate, when to operate, what to do in a particular situation, etc.

- **Detection & Analysis phase:** A hunter is useful in this phase because he/she will be able to assist in the investigation, to determine whether the indicators presented point to an incident or not. The hunter can also assist in obtaining further artifacts that might have been overlooked because the hunter is able to think like an attacker.
- **Containment, Eradication, and Recovery phase:** Hunters have a vast knowledge of various IT domains and IT Security, which allows them to assist in this phase of IR. They can provide recommendations and insight on how the organization can improve its overall security posture. That recommendation can either be a quick implementation or a future implementation.

Risk Assessments

What is a risk assessment?

- A risk assessment is the process of assessing threats, vulnerabilities, and their likelihood of occurring to the organization's assets.
- A risk assessment report will list all the vital systems / processes and the impact to the organization, if anything would happen to these systems.
- This report provides the hunter with an idea as to what systems/processes an intruder would most likely go after. Remember, to be a successful hunter, you must think like the attacker.
- There are other documents that might assist the hunter in determining which systems/processes require more focus than others. Those documents would be a threat
  assessment report or a business impact analysis report.

Threat Hunting Teams

- There is no general definition or description of what ahunting team should be composed of, as organizations determine this based on their size, industry, and

hunger to hunt.

- The three most commonly encountered types are:
  • Ad-hoc hunter
  • Analyst and hunter
  • Dedicated hunting team

Ad-hoc Hunter

- Usually responsible for multiple roles in the organization, and therefore the hunts occur less
  frequently. The hunts are more task-oriented, which requires a clear plan of what to hunt for on a given hunting trip.
- This type of hunter is primarily found in organizations with no formal security team.

Analyst and Hunter

- This type of hunter is the most common, in which SOC analysts also have the responsibility to perform hunting. These skills are complementary; after all, a good hunter is a great analyst.
- This type of hunter is often found in small organizations or those with extremely well-developed detection and baseline capabilities.

Dedicated Hunting Team

- This type of hunter is the most specialized one – a team of a few members whose sole purpose is to hunt. The members are well experienced and qualified.
- This type of hunter is often found in a large organization or governmental organizations.

MODULE 02 | THREAT HUNTING TERMINOLOGY

Threat Hunting Terms

Advanced Persistent Threat

- APTs are groups or nation-states that have a significant amount of resources and infrastructure to conduct their malicious activities. Their targets are in various industries, such as governments, health care systems, and defense systems.
- **Stuxnet** was a cyberweapon – malicious software targeting Iran's nuclear program. It was designed to target Siemens Step7 software on computers controlling a PLC (programmable logic controller).
- Another important point is that APT groups are identified in various ways. One common naming convention is the word APT followed by a number, like APT 1. 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 1 is a Chinese-based cyber espionage group, a nationstate. 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.

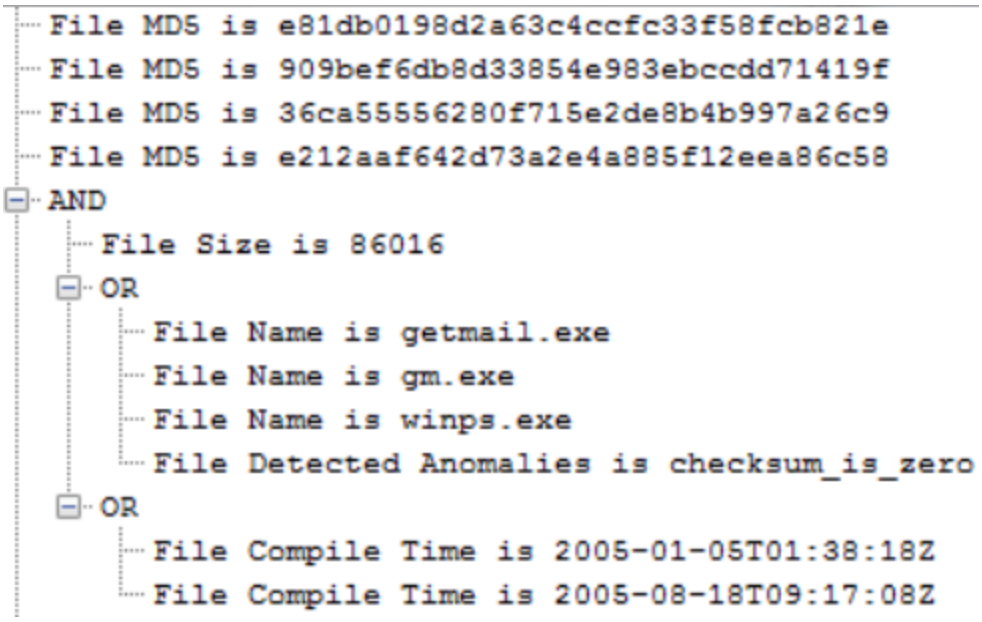
Tactics, Techniques & Procedures

- **Tactics** are the employment and ordered arrangement of forces in relation to each other, which defines the adversary's tactical objective. It is the "why" behind the reason for performing an action.

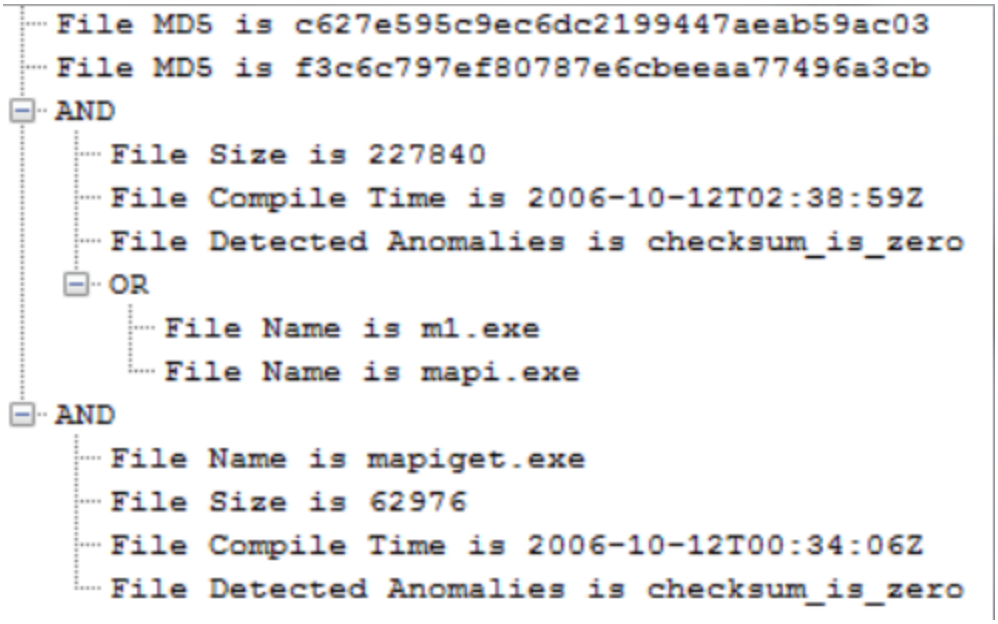
- **Techniques** are non-prescriptive ways or methods used to perform missions, functions, or tasks; this defines "how" the adversary achieves a tactical objective by performing an action.
- Procedures are standard, detailed steps that prescribe how to perform specific tasks. It is the actual implementation of each Technique.
- TTPs will help us identify the adversary in future attacks by creating Indicators of Compromise
  (IOCs).

TTPs - IOCs

- IOCs are artifacts that were gathered from an active intrusion or previous intrusion that are used to identify a particular adversary. These artifacts include MD5 hashes, IP addresses, names of EXEs used, etc.
- For example, we will look at APT 1 and list certain IOCs for APT 1:
  - 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.
  - Here is a snippet of the IOC for GETMAIL.

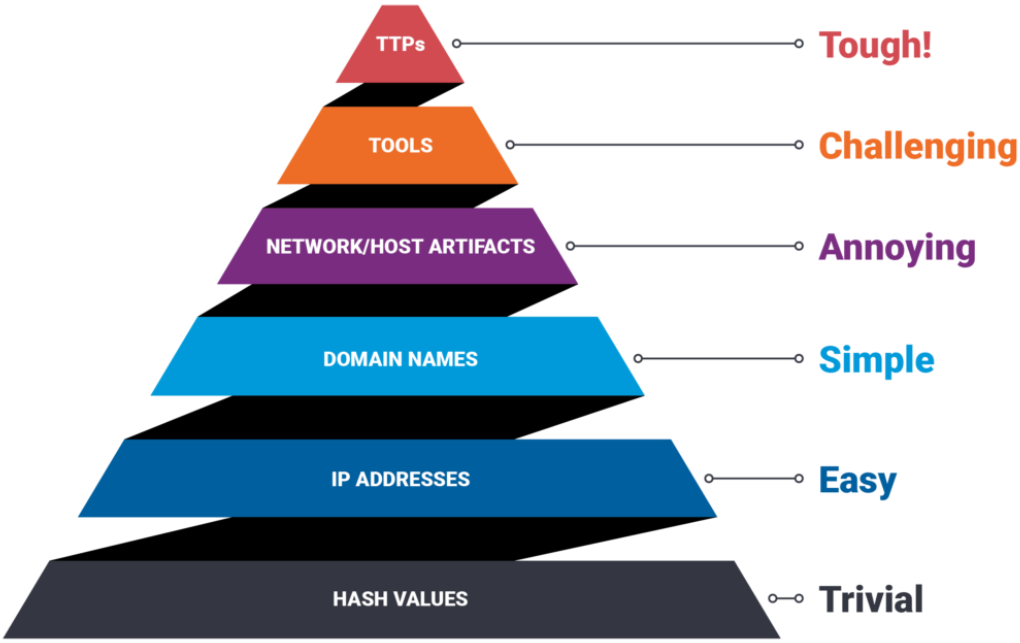


- This is a snippet of the IOC for MAPIGET.



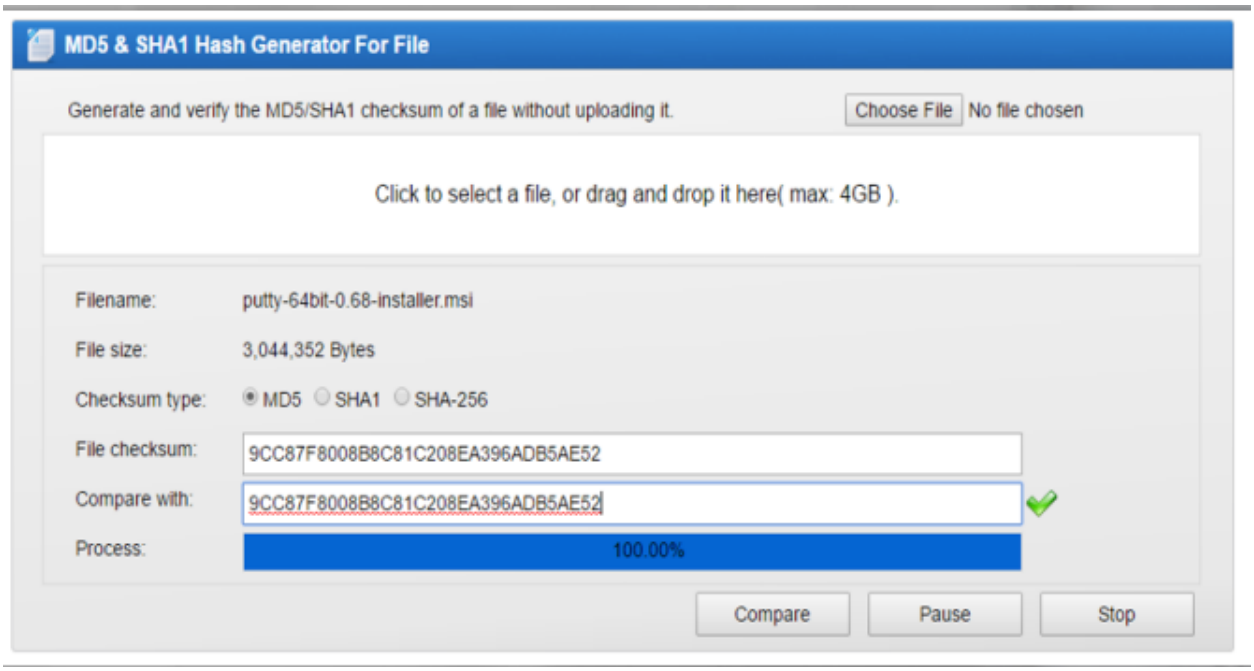
Pyramid of Pain

- Which is a visual that will layer the potential usefulness of indicators that will aid you in detecting an adversary. It also measures how difficult it will be to obtain that particular indicator or indicators, as well as the impact on obtaining the intelligence on them.



Pyramid of Pain – Hash Values

- You might have seen this before when you download a binary (EXE). The developer may 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 the authenticity of the binary you downloaded and verify that it has not been tampered with.
- This screenshot verifies the MSI that was downloaded is authentic based on the checksum
  (MD5) listed on the download page.



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 – 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.
- If the IP addresses are hardcoded, then these IPs can be blacklisted and prevented from making outbound communications; this will make it more difficult for the adversary because now the tools and scripts will have to point to a new IP addresses.

Pyramid of Pain – Domain Names

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

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

What is Punycode?

- From punycoder.com, Punycode is a special encoding used to convert Unicode characters to ASCII. Punycode is used to encode IDNs (Internationalized Domain Names). Below is an example of text in Unicode that is converted to Punycode.

Text	Punycode
Example: 點看	Example: xn--c1yn36f

IDN Homograph Attacks

- In an IDN Homograph Attack, malicious threat actors will exploit the fact that many different characters look alike; this is similar to another concept known as typosquatting.

Legitimate Domain
rvasec.com

Malicious Homograph
rvasec.com

Pyramid of Pain – Network/Host Artifacts

- Network/Host Artifacts are clues the adversary left for us within network packets and on the endpoint systems.

- Below is an example of a Network Artifact and a Host Artifact:

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

- Here we see an example of a network artifact, a fake useragent.

Pyramid of Pain – Tools

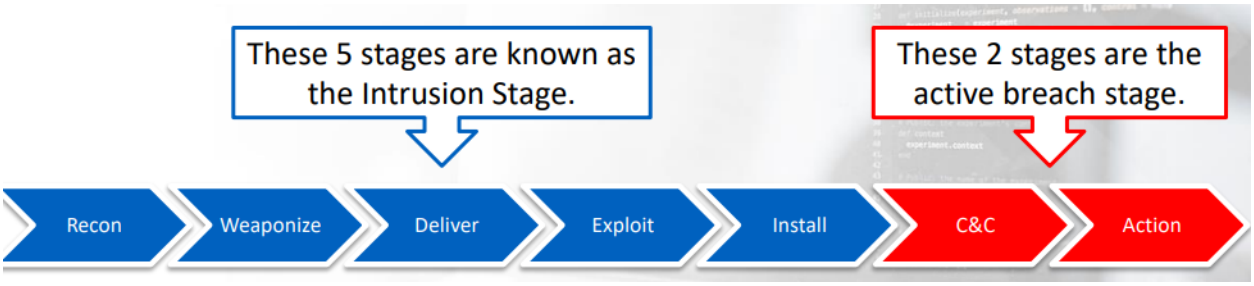
- An APT group will most likely stick to a consistent set of tools. If you're an experienced penetration tester, then you know this to be true. You won't just grab a tool you normally do not use if you're conducting an SQL attack. You will use your tool of preference, such as SQLMap, or something similar.
- If you get good at detecting a particular tool, this will force the adversary to use a new tool. This is because the tool they currently use won't work against your detection capabilities anymore, which will lead to more work on behalf of the adversary.

Pyramid of Pain – TTPs

- The expression of the attacker's training.
- Retraining is hard and expensive. Imagine doing so for 1,000 operators so that the current TTPs and IOCs gathered on them no longer prove to be fruitful. That task is

easier said than done, but if they have the funding, it is not impossible.

Cyber Kill Chain Model



- The **Recon** step involves passive scanning plus OpenSource Intelligence, also known as OSINT (i.e., social media, search engines, etc.). It can also involve active scanning of public-facing IPs.
- **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.
- The **Deliver phase** covers the delivery of the weaponized tool. There are a few methods for delivery, including via email, social media, or a watering hole attack.
- The **Exploit phase** is the actual exploitation, and 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.
- **Install**: At this point, in most cases, additional tools are installed via the RAT. Other tools can be a network scanner, a keylogger, etc.
- **C&C 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 remote access to the compromised machine.
- Action: This is where the goal is achieved. The goal can be exfiltration. This is when:
  • The adversary scans the network, looks for/reviews data, and grabs what they are

looking for.
• What you’re trying to protect leaves the network.

- 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 reconnaissance and look for other machines to exploit.
  • They will also look to cover their tracks.

The 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**.

> 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.

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

Threat Hunting Mindset: Threat Intelligence

- A threat hunter has one of two mindsets. One hunter will rely mostly on indicator-based detection through **threat intelligence**, while the other will rely mostly on technique or anomaly-based detection through **digital forensics**.

What is threat intelligence?

- it is data on threats. The information will come in various forms and could be obtained through multiple channels, such as opensource, social media, vendor reports, etc.

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

Threat Intelligence can be divided into 3 types:

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

Strategic: Who, Why, & Where

- Strategic Intelligence is designed to assist senior management in making informed decisions about the security budget and security strategies (such as risk management).
- Who is the adversary? Why are they targeting you? Where have they attacked prior to attacking you?

Tactical: What & When

- 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, also known as their signature.
- What is the adversary's toolset? When are these attacks orchestrated?

Operational: How

- Deals with the actual indicators, the IOCs, and it addresses the how.
- How is the adversary conducting their attack?

> 💡 Operational Intelligence can merge into Tactical Intelligence. In most cases, you will see it identified as Operational Intelligence.

Threat Hunting Mindset: Digital Forensics

- This hunter will focus primarily on the host, network, and memory forensics in his/her
  hunt when hunting for the unknown.
- They will still use threat intelligence, it would be foolish not to, but this type of hunter will not solely rely on that.

> 💡 Here, we don't wait for an alert from one of the appliances regarding a potential threat. We are proactively hunting!
> This is human-based detection.

- You should also strive to identify variations of a specific attack, not just that one example defined in sources on attack techniques. Think about process masquerading – if a certain attack appears to be running as svchost.exe (except that it is from an odd location), your hunt should aim to expand the detection on other processes that may be victims of this
  type of attack
- With the available data sources, we can choose to perform
  hunts in 2 distinctive ways:
  1. Attack based hunting
  2. Analytics-based hunting

Attack Based Hunting

- we search for evidence whether or not a specific attack has occurred in the environment. We are defining it by asking:
  - Did pass the hash happen in my network?

Analytics Based Hunting

- We look at a set of data and try to see if anything stands out. It is, therefore, crucial to know
  what is normal. We are defining it by asking:
  - Unexpected encryption detected in network traffic

- A receptionist attempting to access HR data

Hunting Periods

- The data utilized in either of the hunting methods can be split into 3 distinctive hunting periods:
  1. Point in Time
  2. Real-Time
  3. Historic

Point in Time

Only detects what is happening on a system at a point in time. It does not identify the activity that
occurred before or after that point in time

Real Time

Detects activity that is occurring in real time. The data collection agent is required to be installed, and the collected data is sent to SIEM. A custom configuration for the collected data is recommended.

Historic

Utilizes logs to identify activities that occurred in the past.

Reverse Engineering Binaries

- The hunter might also reverse engineer binaries, to see if the binary is legitimate or malicious.