The diamond model is a model designed for intrusion analysis that we developed by Sergio Caltagirone, Andrew Pendergast and Christopher Betz in 2013

Composed of four features:

- Adversary
- Infrastructure
- Capability
- Victim

The four core features are edge-connected, representing their underlying relationships and arranged in the shape of a diamond

The diamond model carries the essential concepts of intrusion analysis and adversary operations while allowing the flexibility to expand and encompass new ideas and concepts.

This model can help identify the elements of an intrusion. It can also help non-technical people understand what happened during an even of an attacker

Adversary

Adversary is known as the attacker, The person/group that starts the cyberattack. They are responsible for utilizing a capability against the victim to achieve their intent

It is difficult to identify the adversary at the first stages of a cyberattack. Collecting data from breaches, signatures and other relevant information can help determine who the adversary might be

Adversary Operator - The hacker conducting the attack

Adversary Customer - This is where the person/group may benefit from the cyberattack, which may be the same person as the adversary operator

What is the term for a person/group that has the intention to perform malicious actions against cyber resources?
Adversary Operator

What is the term of the person or a group that will receive the benefits from the cyberattacks?
Adversary Customer

Victim
This is the target of the adversary. A victim could be a person or organisation

A victim will be an opportunity for attackers as they could potentially get a initial foothold on their desired target

Victim Personae - People/Organisations being targeted and attacked. This will include Organisation names, employee names, industries, job roles and much more

Victim Assets - Assets will be the companies data and systems, where the adversary will steal emails, IPs, networks

What is the term that applies to the Diamond Model for organizations or people that are being targeted?
Victim Personae

Capability
Capability is the adversary's Tactics, Techniques and Procedures (TTPs)

These techniques can include from manual process by trying to guess credentials or to automated attacks such as distributing malicious tools

Capability Capacity - Vulnerabilities and exposures that the individual capability can use

Adversary Arsenal - Capabilities that belong to the malicious actor, such as tools

Provide the term for the set of tools or capabilities that belong to an adversary.
Adversary Arsenal

Infrastructure
Known as software or hardware. Physical or logical interconnections that the adversary uses to deliver a capability or maintain control of capabilities

Infrastructure can also be IP address, domains, emails

Type 1 Infrastructure - Controlled or owned by the adversary

Type 2 - Infrastructure controlled by an intermediary

Service Providers - Organisations that provide services considered critical for the adversary availability of type 1 and type 2

To which type of infrastructure do malicious domains and compromised email accounts belong?
Type 2 Infrastructure

What type of infrastructure is most likely owned by an adversary?
Type 1 Infrastructure

Event Meta Features
These are not required but can add some valuable insight. There are 6 possible meta features that can be added:

- Timestamp - Date and time of the event, this can include when the event started and stopped. Timestamps help determine the patterns and malicious activity
- Phase - These are the phase that go back to the cyber kill chain where there are 7 phases to an attack
- Result - This is where the adversary manages to gather their results. This could relate to the CIA
- Direction - Represents host-based and network-based events and represents the direction of the intrusion attack
- Methodology - Allow an analyst to describe the general classification of intrusion
- Resources - Every intrusion event needs one or more external resources to be satisfied to succeed

What meta-feature does the axiom "Every malicious activity contains two or more phases which must be successfully executed in succession to achieve the desired result" belong to?
Phase

You can label the event results as "success", "failure", and "unknown". What meta-feature is this related to?
Result

To what meta-feature is this phrase applicable "Every intrusion event requires one or more external resources to be satisfied prior to success"?
Resources

Social-Political Component
Needs and intent of the adversary, may include financial gain caused by hackers. This may be caused by a computer becoming infected and turning into a botnet

Technology Component

Highlights the relationship between core features; Capability and infrastructure. This is how the attacker will operate and communicate

Practice Analysis

The incident response team has determined that a group of notorious underground hackers named APT2166 are responsible for the attack

Adversary

The attack occurred on 2021-10-23 at 15:45:00:00.000

Timestamp

The attackers targeted the Information Technology (IT) systems of the corporation.

Victim

The attackers used a recent malware campaign known as OneTrick to ransomware the corporation's servers.

Resources

The attackers stole data from the corporation and sold it on an underground hacking forum.

Result

The attackers gained access using legitimate credentials that were gained as a result of a phishing attack.

Capability

Once the attackers gained access to the network, they pivoted to the internal databases and file shares.

Methodology

The attacker’s steps can be followed using the phases of what Cyber Kill Chain model?

Lockheed Martin Kill Chain

Complete all eight areas of the diamond. What is the flag that is displayed to you?

THM{DIAMOND_MODEL_ATTACK_CHAIN}