Sharing Is Caring. If you enjoy this article, help us share with others.

Understanding Diamond Model Of Intrusion Analysis

The Diamond Model of Intrusion Analysis is made up of four parts, as shown in the figure. The model represents a security incident or event. In the Diamond Model, an event is a time-bound activity that is restricted to a specific step in which an adversary uses a capability over infrastructure to attack a victim to achieve a specific result.
The four core features of an intrusion event are adversary, capability, infrastructure, and victim:

- **Adversary** – These are the parties responsible for the intrusion.
- **Capability** – This is a tool or technique that the adversary uses to attack the victim.
- **Infrastructure** – This is the network path or paths that the adversaries use to establish and maintain command and control over their capabilities.
- **Victim** – This is the target of the attack. However, a victim might be the target initially and then used as part of the infrastructure to launch other attacks.

The adversary uses capabilities over infrastructure to attack the victim. The model can be interpreted as saying, “The adversary uses the infrastructure to connect to the victim. The adversary develops a capability to exploit the victim.” For example, a capability like malware might be used over the email infrastructure by an adversary to exploit a victim.

Meta-features expand the model slightly to include the following important elements:

- **Timestamp** – This indicates the start and stop time of an event and is an integral part

of grouping malicious activity.

- **Phase** – This is analogous to steps in the Cyber Kill Chain; malicious activity includes two or more steps executed in succession to achieve the desired result.
- **Result** – This delineates what the adversary gained from the event. Results can be documented as one or more of the following: confidentiality compromised, integrity compromised, and availability compromised.
- **Direction** – This indicates the direction of the event across the Diamond Model. These include Adversary-to-Infrastructure, Infrastructure-to-Victim, Victim-to-Infrastructure, and Infrastructure-to-Adversary.
- **Methodology** – This is used to classify the general type of event, such as port scan, phishing, content delivery attack, syn flood, etc.
- **Resources** – These are one or more external resources used by the adversary for the intrusion event, such as software, adversary's knowledge, information (e.g., username/passwords), and assets to carry out the attack (hardware, funds, facilities, network access).

PEOPLE ALSO READ: 7 Types Of Security Data In Cybersecurity

The figure depicts the Diamond Model as a line drawn diamond. The core features of an intrusion event are located at each of the corners of the diamond.
An adversary is placed on the top, infrastructure is on the left, the victim is on the bottom, and capability is on the right.
There are arrows pointing away from the word adversary at the top to the words infrastructure and capability on the sides, and then arrows pointing from infrastructure and capability to the word victim on the bottom.
The arrows are used to describe the interaction between the core features. The adversary uses the infrastructure to connect to the victim, and the adversary develops a capability to exploit the victim.
Within the diamond is an arrow connecting the adversary and victim and an arrow connecting infrastructure and capability. In the top left of the image is a text list of the Meta-Features; Timestamp, Phase, Result, Direction, Methodology, and Resources.

The Diamond Model

Pivoting Across the Diamond Model

As a cybersecurity analyst, you may be called on to use the Diamond Model of Intrusion Analysis to diagram a series of intrusion events. The Diamond Model is ideal for illustrating how the adversary pivots from one event to the next.

For example, in the figure, an employee reports that his computer is acting abnormally. A host scan by the security technician indicates that the computer is infected with malware. An analysis of the malware reveals that the malware contains a list of CnC domain names. These domain names resolve to a list of IP addresses. These IP addresses are then used to identify the adversary, as well as investigate logs to determine if other victims in the organization are using the CnC channel.

The figure depicts the Diamond Model's Characterization of an exploit. The diamond with the core features is shown, and there are numbered steps with arrows connecting the various core features. Step one connects the victim to the capability, and has the note Victim discovers malware.

Step 2 connects the capability and infrastructure, and has the note Malware contains CnC domain. Step 3 has an arrow arched out from infrastructure to the note CnC Domain resolves to CnC IP address.

Step 4 connects infrastructure to a victim with the note Firewall logs reveal further victims contacting CnC IP address. Step 5 connects infrastructure to an adversary, with the note IP address ownership details reveal adversary

Diamond Model Characterization of an Exploit

The Diamond Model and the Cyber Kill Chain

Adversaries do not operate in just a single event. Instead, events are threaded together in a chain in which each event must be successfully completed before the next event. This thread of events can be mapped to the Cyber Kill Chain previously discussed in the chapter.

The following example, shown in the figure, illustrates the end-to-end process of an adversary as they vertically traverse the Cyber Kill Chain, use a compromised host to horizontally pivot to another victim, and then begin another activity

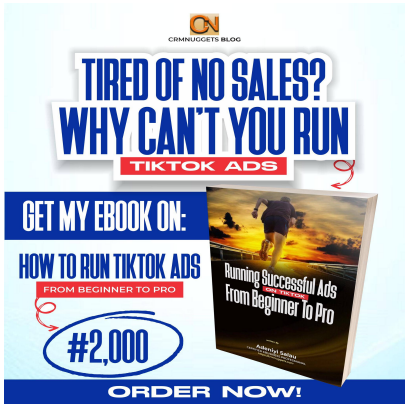
thread:1. Adversary conducts a web search for victim company Gadgets, Inc. receiving as part of the results the domain name gadgets.com.

2. Adversary uses the newly discovered domain gadets.com for a new search "network administrator gadget.com" and discovers forum postings from users claiming to be network administrators of gadget.com. The user profiles reveal their email addresses.

3. Adversary sends phishing emails with a Trojan horse attached to the network

administrators of gadget.com.
4. One network administrator (NA1) of gadget.com opens the malicious attachment. This executes the enclosed exploit allowing for further code execution.
5. NA1's compromised host sends an HTTP Post message to an IP address, registering it with a CnC controller. NA1's compromised host receives an HTTP Response in return.
6. It is revealed from reverse engineering that the malware has additional IP addresses configured which act as a back-up if the first controller does not respond.
7. Through a CnC HTTP response message sent to NA1's host, the malware begins to act as a web proxy for new TCP connections.
8. Through information from the proxy that is running on NA1's host, Adversary does a web search for "most important research ever" and finds Victim 2, Interesting Research Inc.
9. Adversary checks NA1's email contact list for any contacts from Interesting Research Inc. and discovers the contact for the Interesting Research Inc. Chief Research Officer.
10. Chief Research Officer of Interesting Research Inc. receives a spear-phish email from Gadget Inc.'s NA1's email address sent from NA1's host with the same payload as observed in Event 3.
The adversary now has two compromised victims from which additional attacks can be launched. For example, the adversary could mine the Chief Research Officer's email contacts for the additional potential victims. The adversary might also set up another proxy to exfiltrate all of the Chief Research Officer's files.
Note: This example is a modification of the U.S. Department of Defense's example in the publication "The Diamond Model of Intrusion Analysis".

Action Point



Get my 90 Page ebook on How to Run Ads on Facebook. [Click here to buy now.]

PEOPLE ALSO READ: Comprehensive Guide On Use Of SD-WAN

PS: Are you a Nigerian resident abroad and you need to send money to your loved ones back home? The stress is over now! Send money to Nigeria using the MonieWorld app. It's fast, easy and has great rates! MonieWorld is powered by Moniepoint. Sign up with my link

https://spoo.me/iy8taz

P.S.: If you need private online training on any of the ICT courses I offer here and you are in Nigeria, please send me a DM on my WhatsApp at **+2348103180831.** Please note that the Training will be 100percent online. It will be delivered via Zoom or Google Meet.

PS: I know you might agree with some of the points raised in this article or disagree with some of the issues raised.

Please share your thoughts on the topic discussed. We would appreciate it if you could drop your comment. Thanks in anticipation.

Sharing Is Caring. If you enjoy this article, help us share with others.

Related posts:

1. The 10x Daughter. How to be The Star Girl of The Family
2. The 10x Whatsapp Group Administrator . Being a Leader With a Difference
3. The 10x Employee. Building Leaders in Our Organisations
4. Building a 10x Career. The Untaken Path to Career Growth