The Cyber Kill Chain

The Students of Network Security

Why Do We Need It?

- Since the start of the internet age, vulnerabilities have been exploited by ill-meaning users.
- Important data in military and commercial applications were commonly targeted.

Evolving Threats

- Early threats were general viruses with self-replicating code to infect as many things as possible.
- Newer threats are targeted towards specific companies and applications, if not specific users.

When Armor Isn’t Enough

- Network tools allow for hardening and rolling out patches very effectively.
- Targeted malware, zero-day exploitations, and advanced intrusion tools circumvent the hardening.

The Form of the Chain

- US Department of Defense released a paper explaining a kill chain for threats used in the Air Force, a six stage chain.
- Threat chains had been used for IED attacks and threats.

Are Chains Cyber Applicable?

- Information Security professionals had been using phase chain models for a while.
- Attack-Based Sequential Analysis of Countermeasures, Situational Crime Prevention, Exploitation Life Cycle

Topics of the Kill Chain

- The kill chain revolves around incidents, and the information gained from them
- Indicators are used to track incidents and are necessary to use the kill chain effectively.

Indicators

- An Indicator is any piece of information that objectively represents an intrusion.
- Three types of indicators in the Kill Chain context.

The Types of Indicators

- Atomic – An atomic indicator is the smallest an indicator can be cut down to. This can be a IP Address, Email Address, or some other specific vulnerability indicator.

Types of Indicators

- Computed – A computed indicator is an indicator drawn from data involved in an incident. Commonly, computed indicators are hashes or regular expressions.

Types of Indicators

- Behavioral – Behavioral indicators are typically a mix of Atomic and Computed indicators. They can be sentences that explain the sum of the other indicators
- These can help to describe an attack or vulnerability.

Indicator Life Cycle

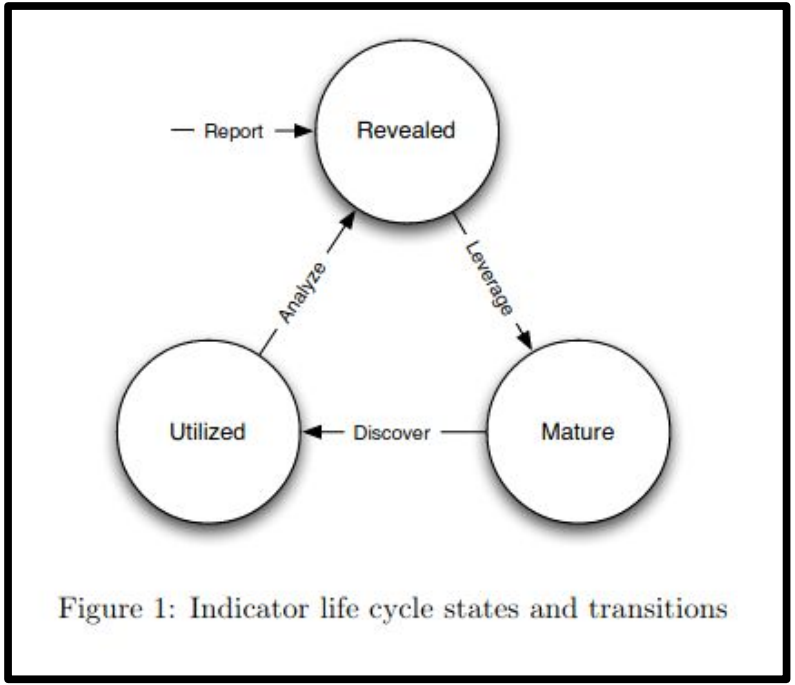

Figure 1: Indicator life cycle states and transitions

What is a Kill Chain?

- A kill chain is a system to procedurally target, engage, and neutralize an adversary.
- The Intrusion Kill Chain is a kill chain specifically focused on a cybersecurity intrusion

The Intrusion Kill Chain

- The stages of the Intrusion Kill Chain are as follows: Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control, and Action on Objectives

Reconnaissance

- This is the identification stage.
- Research, selection, and information gathering make up this stage, focusing on identifying the target.

Weaponization

- This is the preparation phase
- This phase has a focus on making a deliverable payload, focusing on taking some sort of injection and attack and combining them.

Delivery

- This is the deployment phase.
- The transmission of the weaponized payload into the target environment. This typically happens through emails, websites, or removable media.

Exploitation

- This phase executes after the deployment to the host, and the code works to exploit the system.

Installation

- Installation is the payload installing into the target. Typically this is a backdoor or a trojan.

Command and Control

- The payload that has now been exploited would usually beacon back to a remote internet host to establish a channel to communicate through.

Action on Objectives

- After taking the previous six stages, the adversaries can take their actions they had been planning for the entire time.

Late Phase Detection

- Late Phase Detection refers to the threat being detected in the system in one of the later phases of the kill chain, such as Installation or Command and Control.
- Defenders must analyze this and determine future precautions they can take and prepare.

Early Phase Detection

- Early Phase Detection is when defenders find an indicator early on in the kill chain. Typically, early phase detection will come from proper analysis of Late Phase Detection.
- The defenders must predict and infer the final attack to defend the targets later down the chain.

What is a Course of Action Matrix?

- A course of action matrix is a chart detailing responses to an event or intrusion These can detail different stages for each event, and developing solutions into the future.

Stages of a Matrix

- Like the Intrusion Kill Chain, the defenders use the Course of Action Matrix to define their plan.
- The 6 D's (Detect, Deny, Disrupt, Degrade, Decieve, Destroy) are steps the defenders take to stop an intrusion or incident.
- The names of the stages define what the goal of the defenders is.

An Example of a Matrix

Table 1: Courses of Action Matrix

Phase	Detect	Deny	Disrupt	Degrade	Deceive	Destroy
Reconnaissance	Web analytics	Firewall ACL				
Weaponization	NIDS	NIPS				
Delivery	Vigilant user	Proxy filter	In-line AV	Queuing		
Exploitation	HIDS	Patch	DEP			
Installation	HIDS	"chroot" jail	AV			
C2	NIDS	Firewall ACL	NIPS	Tarpit	DNS redirect	
Actions on Objectives	Audit log			Quality of Service	Honeypot	

Application of a Matrix

- When solving an issue, the matrix helps develop security into the future with the same attack vectors.
- The matrix also helps security to develop in a timeline, making security better in the future.

Effectiveness of a Matrix

- By executing the Course of Action Matrix at any given stage of the Intrusion Kill Chain, the attacker's current intrusion gets stopped and cannot continue.
- Stopping any stage of the Kill Chain stops all further stages of that attempt.

Campaign Analysis Basics

- A campaign analysis is where indicators from multiple intrusion attempts line up with each other, and you can determine a single threat causing these attacks.
- There are varying degrees of correlation between attacks.

TTPs

- TTPs are an adversary’s tactics, techniques, and procedures.
- These are used to define the structure and way an adversary works, rather than the specific plan the executed.

How to Use TTPs

- TTPs can be used along with campaign analysis to predict the attack vectors that an adversary will use for further attacks.
- TTPs along with campaign analysis can determine the intent of the attack.

Finale

- Overall, the Cyber Kill Chain has many different parts, and can provide a lot of direction when dealing with an attack.
- Mixing together everything learned here can provide you with tools you need to fend off an attacker, and determine an attack’s direction.

Any Questions?