Pyramid of Pain

Introduction

The Pyramid of Pain is a tiered model that differentiates IOCs based on their value and the level of pain they cause to adversaries when denied.

There are 6 levels in the pyramid of pain

Indicators of compromise (IOCs) refer to data that indicates a system may have been infiltrated by a cyber threat

Hash Values (Trivial)

The hash value is a numeric value of a fixed length that uniquely identifies data

Some of the most popular hashing algorithms are, MD5, and SHA2

Having the hash of a specific malware makes its detection so easy. However, changing the hash is also easy (as easy as just appending one letter to the file)

Tools to check for the hash of a file

https://www.virustotal.com/gui/home/upload

https://metadefender.opswat.com/

Hashes are usually shared at the end of the report to help other professionals in the detection process

IP Address (Easy)

An IP address is used to identify any device connected to a network.

Knowledge of the IP addresses an adversary uses can be valuable. A common defense tactic is to block, drop, or deny inbound requests from IP addresses on your parameter or external firewall.

Changing the IP address is an easy task for an adversary.
This is why IP address is labeled easy

Fast Flux is one of the techniques used to mitigate IP address blacklisting

Domain Name (Simple)

Domain Names can be thought as simply mapping an IP address to a string of text.

Domain Names can be a little more of a pain for the attacker to change as they would most likely need to purchase the domain, register it and modify DNS records.

To detect the malicious domains, proxy logs or web server logs can be used.

Attackers usually hide the malicious domains under URL Shorteners.

You can see the actual website the shortened link is redirecting you to by appending "+" to it

Host Artifacts (Annoying)

Host artifacts are the traces or observables that attackers leave on the system, such as registry values, suspicious process execution, attack patterns or IOCs (Indicators of Compromise), files dropped by malicious applications, or anything exclusive to the current threat.

Network Artifacts (Annoying)

A network artifact can be a user-agent string, C2 information, or URI patterns followed by the HTTP POST requests.

The User-Agent is defined by RFC2616 as the request-header field that contains the information about the user agent originating the request.

Network artifacts can be detected in Wireshark PCAPs

Network protocol analyzers like TShark or Snort can help in identifying out of the ordinary user-agent strings

Tools (Challenging)

Tools are any software (i.e. any custom .EXE, and .DLL files) used by the adversary to accomplish their mission

In this level, the attacker would most likely give up trying to break into your network or go back and try to create a new tool that serves the same purpose.

Antivirus signatures, detection rules, and YARA rules can be great weapons to use against attackers at this stage.

Good resources for samples, malicious feeds, and YARA results

https://bazaar.abuse.ch/

https://malshare.com/

https://tdm.socprime.com/ Good resource for detection rules

Fuzzy hashing helps you to perform similarity analysis - matching two files with minor differences based on the fuzzy hash values.

Tools:
https://ssdeep-project.github.io/ssdeep/index.html

TTPs (Tough)

TTPs stands for Tactics, Techniques & Procedures. This includes the whole MITRE ATT&CK Matrix, which means all the steps taken by an adversary to achieve his goal, starting from phishing attempts to persistence and data exfiltration.

If you can detect and respond to the TTPs quickly, you leave the adversaries almost no chance to fight back.