



CS-501

Introduction to Malware, Threat Hunting &
Offensive Capabilities Development

Lecture 1: Basics of Real Life Threat Analysis

Learning an entirely new language

Definitions are important

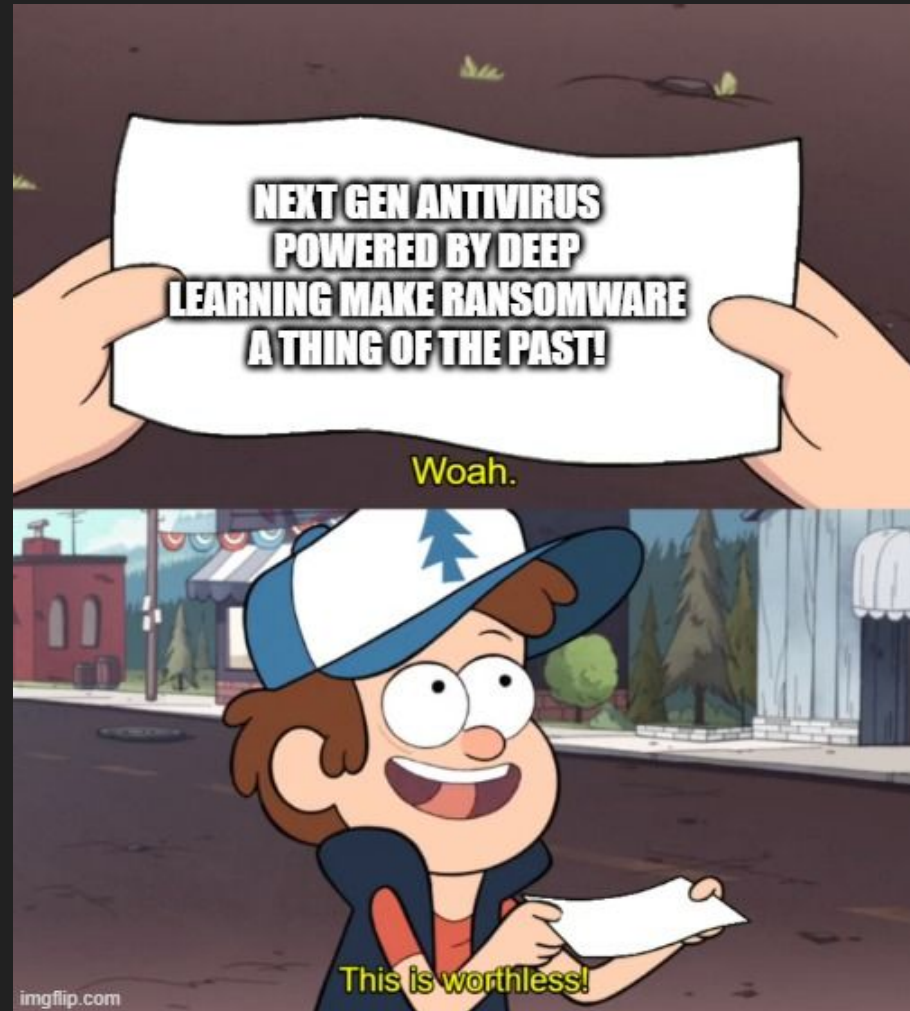
Specialist language allows people to be specific.

Industry is full of jargon, and knowing your definitions makes you less susceptible to snake oil salesmen.

It also allows you to communicate more precisely.

Unfortunately, unlike Mathematics, there really isn't a single (trustworthy!) authority.

In fact, many orgs cook up their own!



Definitions

Malware

Threat Hunting

Offensive Cyber Capabilities

Definitions

Malware: malicious software [has a bunch of definitions, can get very meta]

At the end of the day, it is code that “does a thing” that the person who ran it might not either expect or want.

Context matters. Is PSEXEC Malware? Is Slack malware? Is RDP malware? Is Exchange Malware?

Definitions










What makes malware different from antivirus?

How is a “rootkit” different from a driver that monitors your PC?

Is CrowdStrike malware with good marketing?

Meme src:

https://twitter.com/___winn

MALWARE ALIGNMENT CHART			
	DOCTRINE PURIST	DOCTRINE NEUTRAL	DOCTRINE RADICAL
	Malware is deployed on a target machine.	Malware is deployed in a target environment.	Malware has a target.
STRUCTURE PURIST Malware has harmful effects on software or hardware.	 WannaCry is malware.	 An airstrike is malware.	 A hammer is malware.
STRUCTURE NEUTRAL Malware has unintended effects on software or hardware.	 McAfee Antivirus is malware.	 Squirrels in power grids are malware.	 Power outages are malware.
STRUCTURE RADICAL Malware has an effect.	 Microsoft OWA is malware.	 Roombas are malware.	 Emails are malware.

Definitions

Malware: malicious software

[has a bunch of definitions, can get very meta]

Threat Hunting: Searching environments to detect and isolate malicious activity.

Definitions

Malware: malicious software

[has a bunch of definitions, can get very meta]

Threat Hunting: Searching environments to detect and isolate malicious activity.

- **Blue Team:** Analysis/Detection of new malicious activity, creating detection rules, attribution.
- **Red Team:** Attribution re: attacker environments, and/or emulation of real malicious activity.

There are other team “colors” that we do not cover in this class.

Definitions

Malware: malicious software

[has a bunch of definitions, can get very meta]

Threat Hunting: Searching environments to detect and isolate malicious activity.

- **Blue Team:** Analysis/Detection of new malicious activity, creating detection rules, attribution.
- **Red Team:** Attribution re: attacker environments, and/or emulation of real malicious activity.

Offensive Cyber Capabilities: lots of definitions here - for this class, we'll call it "anything related to the internet that allows an attacker to infiltrate victim computers / networks".

Cyber Operations 101

Many types of actors conduct cyber operations

Criminals

Hacktivists

Mercenaries/Private Industry

Literal children

Government/Government backed Actors (APTs)

Many types of actors conduct cyber operations

ADVANCED PERSISTENT THREATS (APTs): usually associated with nation state actors, but any actor conducting cyber operations that can consistently target a set of victims and succeed can fall under this category.

Large criminal groups with tacit government approval/protection (FINs)

Cyber Mercenaries / Contractors (APT3 -> Boyusec, Appin Security, Positive Technologies, NSO Group)

Government Intelligence Agencies (FSB -> APT29, RGB -> Lazarus Group, NSA TAO → Equation/G0020)

Why conduct cyber operations?

Activism (DDoS attacks to shut down Nazi sites, defacing government websites)

Crime (Ransomware, stealing credentials, installing coin miners)

Espionage [CNE] (commercial vs. geopolitical -> stealing Intellectual Property / state secrets)

“Warfare” [CNA] (Shutting down a country’s internet, disrupting power grids, making nuclear centrifuges spin too fast, etc).

Clout/Trolling/fun Go to Shodan.io and search for sites with an HTML title “Hacked by*”

Why conduct cyber operations?

Activism (DDoS attacks to shut down Nazi sites, defacing government websites)

Crime (Ransomware, stealing credentials, installing coin miners)

Espionage [CNE] (commercial vs. geopolitical -> stealing IP / state secrets)

“Warfare” [CNA] (Shutting down a country’s internet, making nuclear centrifuges spin too fast, etc).

Some actors do a mix

North Korea:

- Bank heists
- Ransomware attacks
- Hack & Leak
- Destructive malware
- Espionage

Img: <https://www.bbc.com/news/stories-57520169>



Example 1: OPM hack

Target: Gov

Attacker: Gov (espionage)

Benefit: intel/counterintel



“The compromised data included SF-86 forms which contain intimate details about the prospective employee’s personal life, family members, and other contacts.”

Example 2: Twitter hack

Target: Corporation/Individuals

Attacker: Users / Individuals

Benefit: Ego + Money

What else could he have done?



We are giving back to our community. We support Bitcoin and we believe you should too!

All Bitcoin sent to our address below will be sent back to you doubled!



Only going on for the next 30 minutes.

Example 3: stalkerware

Target: User

Attacker: User

Benefit: surveillance/ Ego

Is “Find my friend” Malware?

What about location services?



Example 4: Jamal Khashoggi Assassination

Target: Individual

Attacker: Foreign Government + Mercenary

Benefit: Political



Example 5: Advertising

Target: User

“Attacker”: Company

Benefit: Money

Note Facebook and Google are not intelligence companies. A running joke is the intelligence community (IC) is jealous of the digital marketing industries surveillance capabilities



Example 6: SaltStack RCE

Target: LineageOS, Ghost, DigiCert (anyone vulnerable to a specific exploit)

Attacker: various

Benefit: Financial

What else could they have done?

<https://thehackernews.com/2020/05/saltstack-rce-exploit.html>



Malware 101

What platforms does Malware target?

Anything that can run code is susceptible to malware



Definitions: Common types of malware

Packer: a tool that compresses, encrypts, and/or modifies an executable usually for the purpose of defense evasion .

Loader / Dropper: software that downloads and executes other **malicious** programs.

Spreader/Worm: software designed to spread **malicious** content on the system/executes the first of the attack. A virus.

Miner: malicious software that mines cryptocurrency on a victim machine.

Locker/Wiper: malware that encrypts/destroys files on a victim machine .

Backdoor: Similar to a loader/dropper but specifically designed to regain access

Spyware/RAT: collections of tools designed to spy on the victim machine that usually controlled by a remote server.

Stealer: Similar to spyware, but generally pillages a computer for all available passwords, crypto wallets...etc and exits.

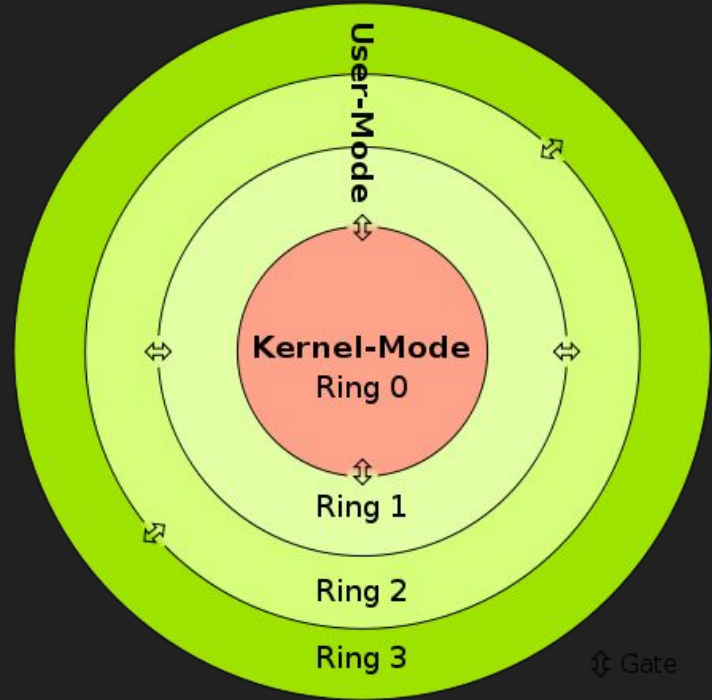
Implant: catch all term for malware “implanted” on a victim machine

Definitions: Less common types of malware

Rootkit: Generally speaking this is a subclass of spyware. Rootkits are deployed on victim machines that usually have been “rooted” or where the attacker has escalated their privileges on the device. They usually try to hide their existence by hiding (among other things) processes, network traffic/connections, and files from the OS. Subclasses are defined based on what ring they run in.

Is a debugger a rootkit?

What about Riot Game’s Anti Cheat engine for Valloran?



C2 / Command and Control

Malware is just code. It is created to perform a job, and usually takes its marching orders from, and sends job results to remote servers

We call these servers Command and Control Servers (C2s)

We call the mechanism that sends data to and from C2 servers the **C2 Channel**

Note some malware is autonomous (Wanacry)

Some malware uses P2P communication (Game Over Zeus)

Some malware is deployed as a larger “Post Exploitation” effort

Examples of C2 Channels

TCP

UDP

ICMP

HTTP(s)/ HTTP2/HTTP3

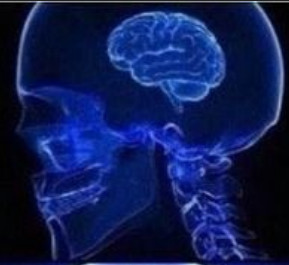
DNS

TLS handshakes/heartbeats

Trusted 3rd Parties

Other “Exotic” methods

**SENDING COMMANDS
TO BOTS VIA
A REVERSE TCP SHELL**



**SENDING DATA
VIA HTTPS DISGUISED
AS WEB TRAFFIC**

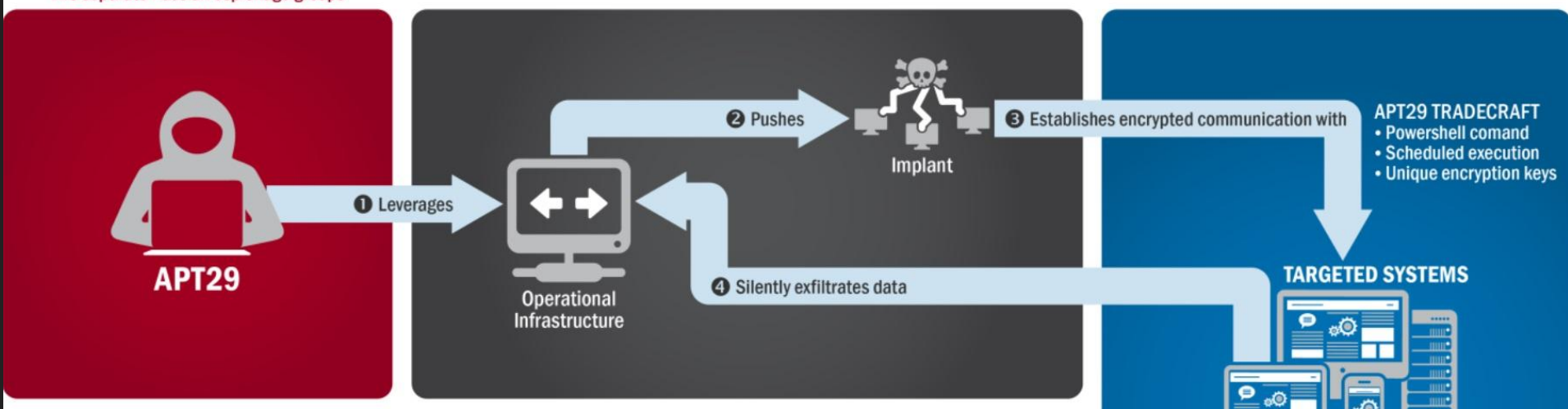


**TUNNELING
DATA USING DNS
AND AAAA RECORDS**



**CONTROLLING
BOTS BY COMMENTING
ON BRITNEY
SPEAR'S INSTAGRAM**





Two separate Russian espionage groups



APT29

① Leverages



Operational
Infrastructure

② Pushes



Implant

③ Establishes encrypted communication with

APT29 TRADecraft

- Powershell comand
- Scheduled execution
- Unique encryption keys

④ Silently exfiltrates data

TARGETED SYSTEMS



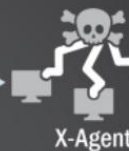
APT28

① Leverages



Operational
Infrastructure

② Deploys



X-Agent

③ Installs onto

④ Leverages



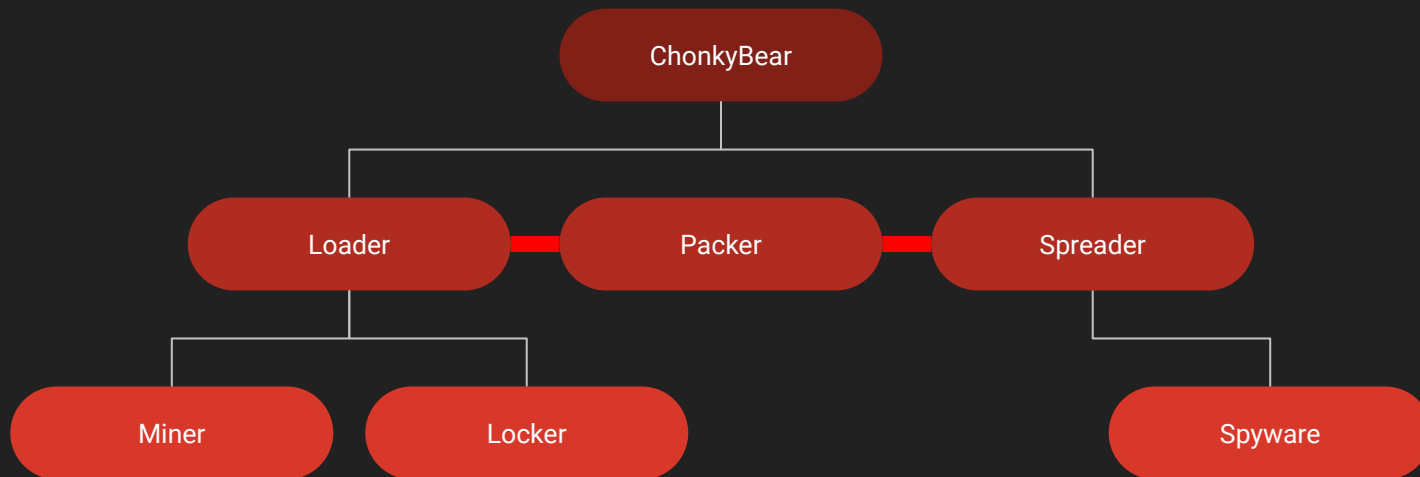
X-Tunnel

⑤ Enables remote execution

APT28 TRADecraft

- Remote execution
- File transmission
- Keylogging

APT ChonkyBear



How does Cyber Threat Analysis / Threat Hunting Work?

Goal of Threat Hunting

Threat Hunting: Searching environments to detect and isolate malicious activity.

- **Blue Team:** Analysis/Detection of new malicious activity, creating detection rules, attribution.
- **Red Team:** Attribution re: attacker environments, and/or emulation of real malicious activity.

Goal of Threat Hunting

Threat Hunting: Searching environments to detect and isolate malicious activity.

- **Blue Team:** Analysis/Detection of new malicious activity, creating detection rules, attribution.
 - Finding new phishing emails, figuring out who is targeting your company and why, figuring out how to block malware or the emails from getting to your inbox in the first place.
- **Red Team:** Attribution re: attacker environments, and/or emulation of real malicious activity.
 - Finding out there's a bunch of phishing emails that compromised another company in your industry, and emulating the attack on your own company to see if it succeeded.

Quick Remark about Ethics and Red Team

Example: Emulating phishing activities of a financially motivated actor.

Consider a threat actor that sends targets a malicious document with a lure that uses one of the following email templates:

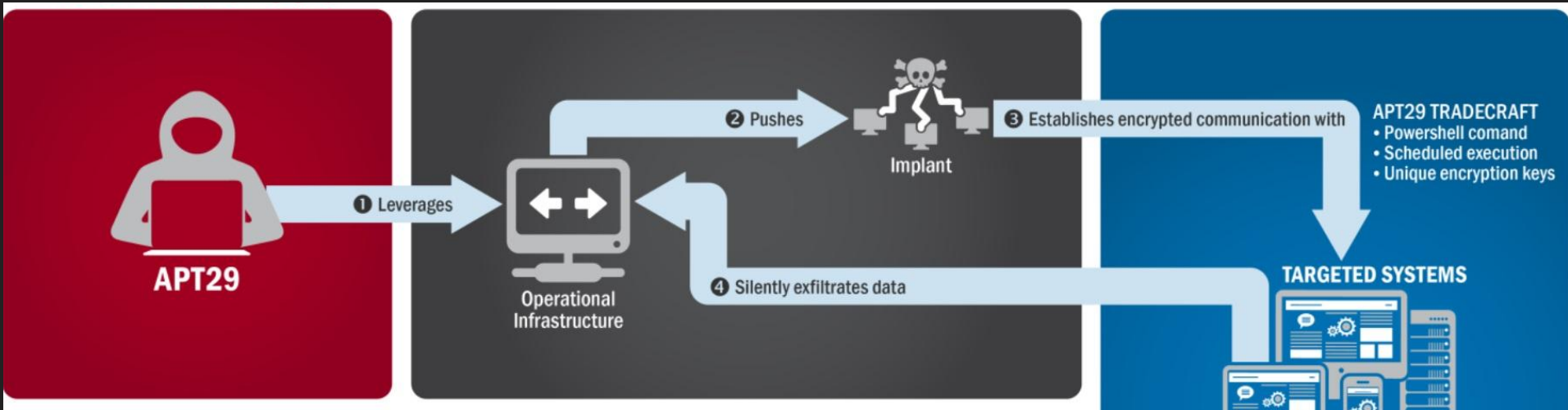
- 1) WARNING: You came into contact with someone with COVID-19!
- 2) URGENT: Immediate termination of your Position
- 3) Due to the hardship of COVID-19, we are issuing a one time spot bonus of \$5000

Should you emulate these tactics by sending your employees simulated emails using the templates above?

DON'T BE THAT PERSON

No. Seriously, don't stress out your employees over something that isn't going to make them safer.

The attackers won't play by the rules you lay out, but you should not try to emulate everything that they do.



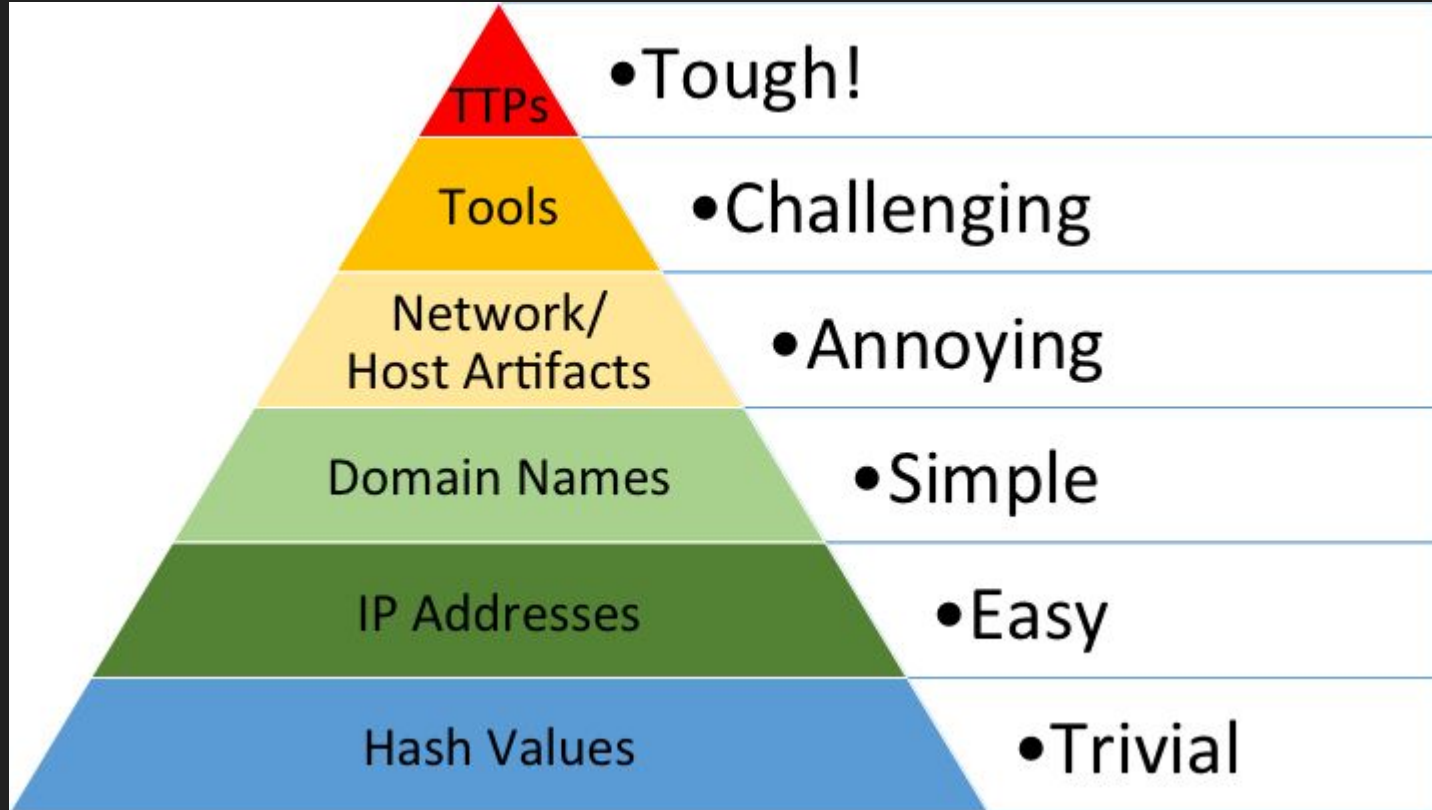
Blue team: how do I make sure this attacker can't successfully compromise our network?

Red team: how do I pretend to be this attacker to test under what circumstances we get past the blue team?

How do you do this?

- Finding Indicators of Compromise
- Moving from Indicators of Compromise (IOCs) -> Tactics, tools and procedures (TTPs)
- Protecting your Environment from the Tactics / Tools / Procedures used.
- Breaking Links in the “cyber killchain”

Threat Analysis Pyramid of Pain



More Definitions

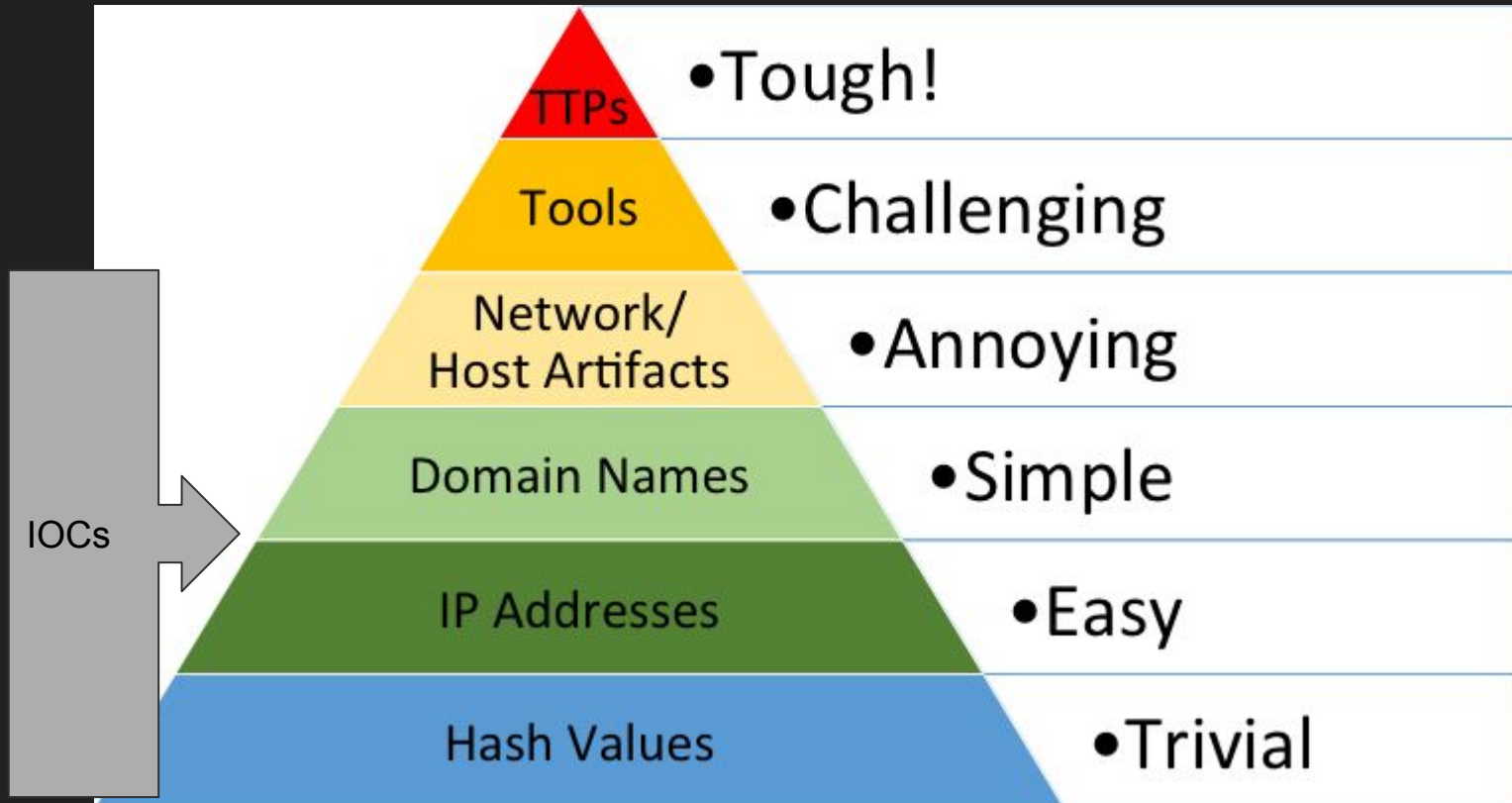
Hash value: the unique fingerprint of a single file

IP address: the unique address of a computer on a network.

Domain Name: the unique name of a website on the internet.

Indicators of Compromise (IOCs): sets of forensic data found when malicious activity occurs. (IPs / domains of a C2 server, hash values of malware, email accounts of phishing email senders..etc)

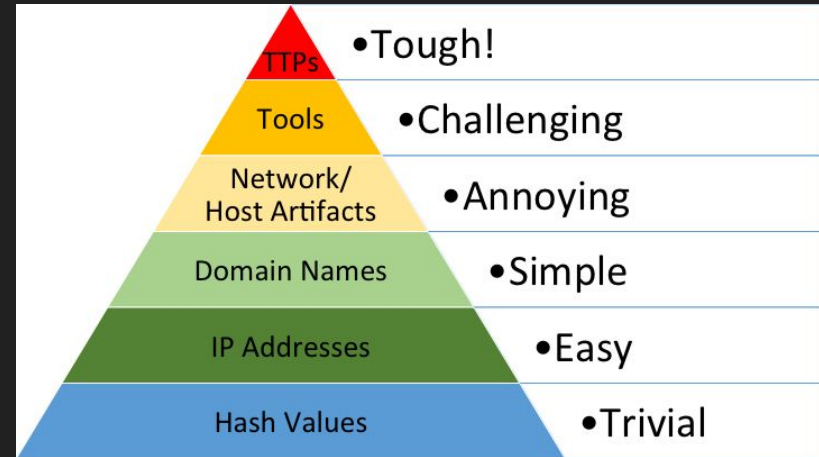
Threat Analysis Pyramid of Pain



Threat Analysis Pyramid of Pain

Getting from IOCs -> TTPs:

- **Hash -> Tools:** What malware family does this hash belong to? How are all these hashes similar? Can I block every instance of the malware?
- **IP/Domain -> Network Artifact:** How does the malware communicate with the C2? Can I look at common patterns in the network traffic and block that behavior?
- **IOC -> TTPs:** Is there a pattern in the way this group conducts operations? Do they drop multiple malware families? Do they look for specific data? How do I block this activity?



Like all things, it depends

Depending on the actor, the Pyramid of Pain might just be pain.

Hashes are easy, **unless they use polymorphic code**

IPs are easy, **unless they use thousands of addresses all of which are compromised infrastructure**. Hint: what happens when someone takes over a Kubernetes cluster or an admin cloud account?

Domains are easy, **unless they use a domain generating algorithm (DGA) or quickly change them**.

Different companies see different IOCs

Antivirus companies (Norton, McAfee) see the malware that attackers use.

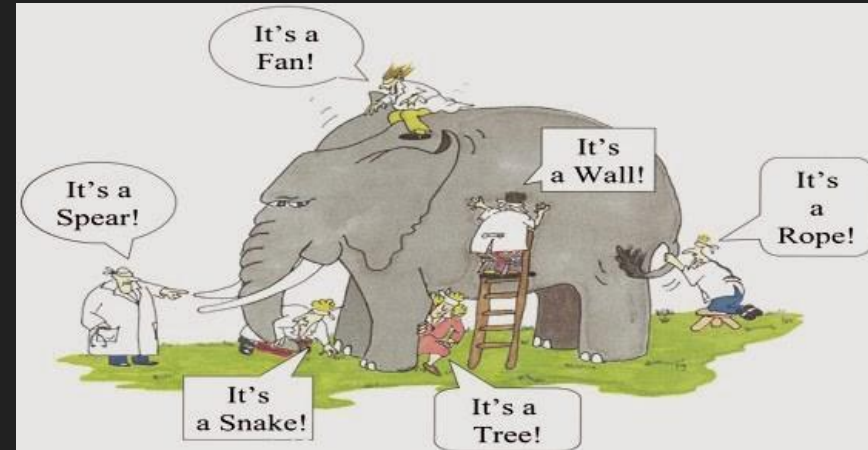
Mail providers (Gmail, Yahoo) see the phishing emails.

Domain registrars (Namecheap / GoDaddy) see Command and Control registration.

Nobody sees everything.

Analysis is hard.

You're going to have to work as a team.



Remark on Infosec Savants

There are plenty of brilliant people working in infosec, but by and large there is no such thing as someone who has all the answers.

In fact, someone who claims they do is likely wrong, lying, or trying to sell you something.

There is no Infosec Dr. House. It's probably just someone with a bit too much self confidence, and they probably are not fun to work with.

Cybersecurity is a team sport.



How are we doing this in class?

Class Progression (blue team side)

Analysing Malware - *(pulling out the IOCs in the malware)*

- Example Assignment: Find all C2 domains, interesting files, and implant configuration,

Writing up a Technical Report on the Malware - *(explaining the IOCs and how the malware works)*

- Example Assignment: What is the malware trying to accomplish?

Creating Threat Hunting Rules to find more malware

- Example assignment: finding all code associated to APT Chonky bear in a collection of binaries

Class Progression (blue team side)

Analysing First stage loaders: Analysing Malware - *(pulling out the IOCs in the malware)*

Writing up a Technical Report on the Malware - *(explaining the IOCs and how the malware works)*

Creating Threat Hunting Rules to find more malware

Homework Discussion

What do we need to control a computer?