CS-501

Introduction to Malware, Threat Hunting
& Offensive Capabilities Development

Reminder:
CFAA is a a big hammer.

Today in CFAA

- American Airlines is suing The Points Guy for syncing account data *with* user consent
- According to AA, this constitutes widespread hacking.
- AA is using the CFAA for its lawsuit.
- The CFAA is vague enough where AA might get what they want
- Either through a sympathetic judge's interpretation, or by prolonged and expensive litigation.

American Airlines suing The Points Guy over app that syncs frequent flyer data

The airline claims the travel tips site is violating its terms of use and infringing its trademarks

By Kim Lyons | @SocialKimLy | Jan 21, 2022, 5:58pm EST

SHARE

Lecture 1:
Basics of Real Life Threat Analysis
Learning an entirely new language

Definitions are important

Specialist language facilitates precise communication about complex topics.

Infosec is full of technical jargon and corporate speak.

It is also full of marketing teams that make up their own jargon.

Definitions are important

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

There are efforts in place to standardize vocabulary, but you will likely have context dependent jargon depending on where you work.

Military folks, Intelligence community vets, policy wonks, hackers and Punks, all have their own culture, definitions, and slang.

You will encounter folks with all kinds of ideas and political beliefs.

Many of whom have large platforms. Some with really bad takes dressed up in legitimizing jargon.

HAWKISH POLICY CRANKS ON TWITTER EXPLAINING WHY PORT SCANNING SHOULD BE A CAPITAL OFFENSE

ME TRYING TO FIND THE CAT IN A "THERE IS NO CAT IN THIS IMAGE"

BS Detector

Seriously, having a good nose for BS will go a long way. Infosec is saturated with it.

Infosec is especially tricky, as it evolves rapidly.

Many people (myself included) constantly feel like they are behind the curve and playing catch up.

Marketers capitalize on this to make you feel out of the loop :)

Technical Definitions

Malware

Threat Hunting

Offensive Cyber Capabilities

Definitions

Malware: Unwanted, malicious software.

It has a bunch of definitions, and 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? Is Crowdstrike's EDR malware?

Common activities performed by malware

- Host enumeration: whoami, whereami, whatami
- Network enumeration: what can I talk to, where can I get to?
- Execute: Powershell, Batch, shellcode…etc
- Download: get data into the computer
- Exfiltrate: get data out of the computer
- Process Manipulation: start, list, modify, and kill processes
- External Messaging: communicate with an external server

Are these indicators of a malicious program?

Wacom drawing tablets track every app you open

But there's a way to disable it.

in   F   f   y   ✉

Written by **Catalin Cimpanu**,
Contributor

Posted in Zero Day on February 6, 2020 | Topic: Security

https://www.zdnet.com/article/wacom-drawing-tablets-track-every-app-you-open/
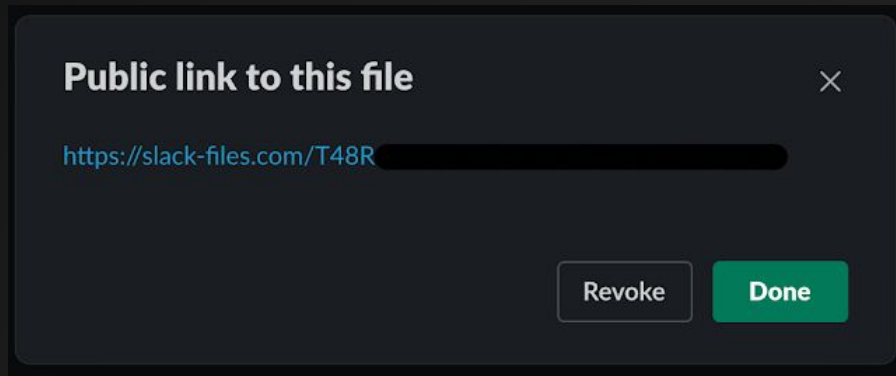
Malware is Subjective

The line between analytics and marketing and spyware can get blurred pretty quickly

Is Slack Malware

- Slack is a messaging service
- Slack allows you to host static files of any type and create public download links.
- Slack lets you script communication in its messenger, and can be used as a communication channel

https://threatpost.com/attackers-discord-slack-malware/165295/

Public link to this file   ✕

https://slack-files.com/T48R▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇▇

Revoke Done

PSExec: Goodware?

- PSExec is a utility from the sysinternals suite of tools.
- It is used to execute powershell commands/scripts on a remote machine and is incredibly useful for sysadmins
- It is also commonly used in offensive cyber operations
  - Note that it is less common now because it became the default method for many popular tools, and vendors got good at flagging it.
  - It is still commonly used by crimeware.

https://www.mandiant.com/resources/a-nasty-trick-from-credential-theft-malware-to-business-disruption

The following high-level steps appear common across most incidents into which we have insight:

- Actors produce a list of targets systems and save it to one or multiple .txt files.

- Actors move a copy of PsExec, an instance of Ryuk, and one or more batch scripts to one or more domain controllers or other high privilege systems within the victim environment.

- Actors run batch scripts to copy a Ryuk sample to each host contained in .txt files and ultimately execute them.

15

Is Crowdstrike's Agent Malware (Falcon)

Short answer: No…well kind of but don't seriously no.

It acts a lot like malware does! If you ever gain control of a company's Falcon endpoint, they are probably screwed!

Falcon is a a set of tools designed to "stop breaches"

It does so by gathering telemetry, spying on processes, and alerting/responding to activity it deems malicious.

https://github.com/Mr-Un1k0d3r/EDRs/blob/main/EDRs.md

Definitions

What makes malware different from an antivirus?

How is a hacked exchange server any different from a dedicated malicious server?

Is Crowdstrike malware with (really) good marketing?

Meme src: https://twitter.com/__winn

MALWARE ALIGNMENT CHART

	DOCTRINE PURIST Malware is deployed on a target machine.	DOCTRINE NEUTRAL Malware is deployed in a target environment.	DOCTRINE RADICAL 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.

Quick remark about Weird Machines

What if I execute malicious code only using instructions inside of a legitimate program?

Is PDF parser malware?

Recommended reading:

https://googleprojectzero.blogspot.com/2021/12/a-deep-dive-into-nso-zero-click.html

Definitions

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

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

Definitions (for this class)

Malware: Unwanted, 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

Red Team Engagement: An exercise involving (ideally) an external entity that provides continuous testing and validation of security controls for an organization.

While not totally accurate, it can be a useful starting point to think of a red team engagement as an open scope penetration test.

I.e., the folks carrying out the exercise will more open rules of engagement. This definition can also get very meta, and is borrowed from military jargon.

ROE: What am I, the (fake) attacker, allowed to do during this exercise?

Definitions

Blue Team: an internal entity responsible for detecting, and remediating security incidents.

These are the folks who work around the clock to catch red teamers in addition to real threats.

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.

Definitions

Offensive Cyber Capabilities

For this class, we'll define it as "A device or computer that allows an adversary to execute on an objective during a cyber operation."

Note this can also get very meta.

Example: wiper malware that destroys computers used by mass transit

Non-Example: firing a rocket at an AWS datacenter to take everyone offline.

Grey Area: sending Neurolink super squirrels to chew networking cabling.

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 Government 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?

Does social engineering count as
an offensive cyber capability?

Example 3: Monitoring

Target: User(s)

Attacker: Organization

Benefit: surveillance

Is "Find my friend" Malware?

What happens if someone compromises GoGuardian?

Example 4: Jamal Khashoggi Assasination

Target: Individual
Attacker: Foriegn Government +
Mercenary
Benefit: Political

Example 5: Advertising

Target: User

"Attacker": Company

Benefit: Money $$$$$

Remember Wacom? They were using Google Analytics

Note Facebook and Google are not intelligence companies per say.

That said, they collect data that the intelligence community (IC) would kill for.

Make no mistake, digital marketing companies have impressive surveillance capabilities

Example 6: Opportunistic Mass Exploitation

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

Monero Botnet

Literally everything connected to the internet

imgflip.com

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?

User-Mode

Kernel-Mode
Ring 0

Ring 1

Ring 2

Ring 3

⇕ Gate
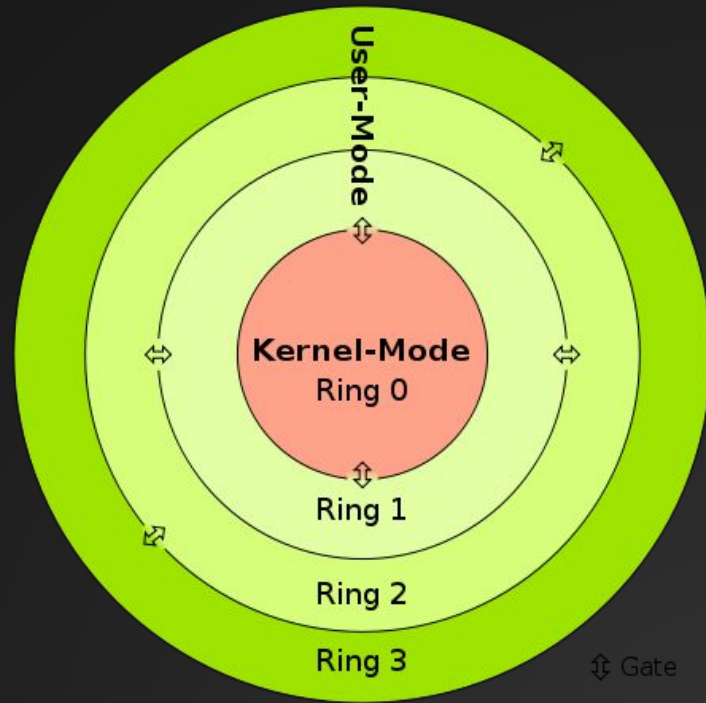
C2 / Command and Control

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

imgflip.com

Two separate Russian espionage groups

APT29

① Leverages → Operational Infrastructure

② Pushes → Implant

③ Establishes encrypted communication with

④ Silently exfiltrates data

APT29 TRADECRAFT
• Powershell comand
• Scheduled execution
• Unique encryption keys

TARGETED SYSTEMS

43

Two separate Russian espionage groups

APT29

Operational Infrastructure

1 Leverages

2 Pushes

Implant

3 Establishes encrypted communication with

4 Silently exfiltrates data

APT29 TRADECRAFT
• Powershell comand
• Scheduled execution
• Unique encryption keys

TARGETED SYSTEMS

APT28

Operational Infrastructure

1 Leverages

2 Deploys

X-Agent
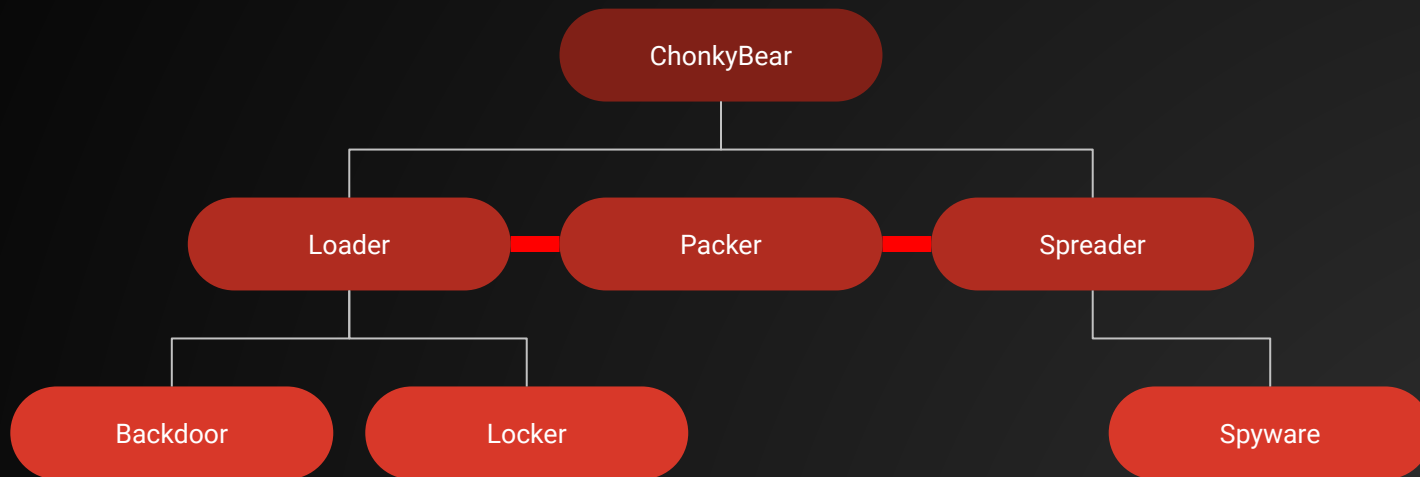
3 Installs onto

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.
  - Identifying the actors who carried out the phishing campaign

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 aboe?

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.
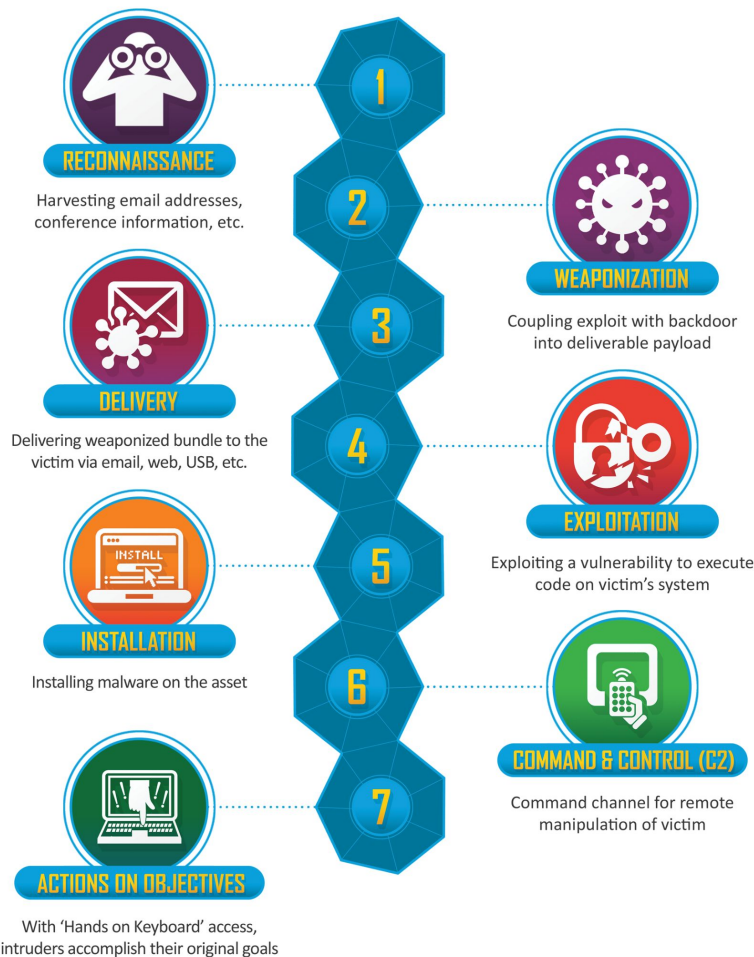
Frameworks for talking about Cyber Operations

There are a lot. Two of the more popular ones are

1) Lockheed Martin Cyber Kill Chain
2) MITRE ATT&CK

Cyber Killchain

- Framework for identifying the steps an adversary takes to execute on a tactical objective
- As defenders, if you can "break a link in the chain" you can disrupt an adversaries operation

RECONNAISSANCE
Harvesting email addresses, conference information, etc.

2 WEAPONIZATION
Coupling exploit with backdoor into deliverable payload

3 DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.

4 EXPLOITATION
Exploiting a vulnerability to execute code on victim's system

5 INSTALLATION
Installing malware on the asset

6 COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim

7 ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

MITRE ATT&CK

- Similar approach to Cyber Killchain
- Goes into detail about specific TTPs: Tactics, Techniques, and procedures
- Is an industry standard for talking about how an objective was achieved or how an action was performed
- https://attack.mitre.org/matrices/enterprise/
- https://attack.mitre.org/resources/faq/
- This course takes many of its definitions from MITRE
- It is far from a perfect framework, but it is another (incredibly useful) tool in your arsenal

TTPs: Tactics

"Tactics represent the 'why' of an ATT&CK technique or sub-technique. It is the adversary's tactical goal: the reason for performing an action. For example, an adversary may want to achieve credential access."

Example: Disrupting Iran's nuclear program

TTPs: Techniques

"Techniques represent "how" an adversary achieves a tactical goal by performing an action. For example, an adversary may dump credentials to achieve credential access."

This includes the tools used, and you will sometimes hear me slip up and say *tactics tools and procedures*

TTPs: Sub-Technique

"Sub-techniques are a more specific description of the adversarial behavior used to achieve a goal. They describe behavior at a lower level than a technique. For example, an adversary may dump credentials by accessing the Local Security Authority (LSA) Secrets."

TTPs: Procedures

"Procedures are the specific implementation the adversary uses for techniques or sub-techniques. For example, a procedure could be an adversary using PowerShell to inject into lsass.exe to dump credentials by scraping LSASS memory on a victim. Procedures are categorized in ATT&CK as the observed in the wild use of techniques in the 'Procedure Examples' section of technique pages."

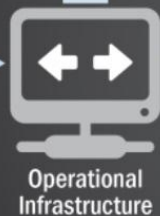I like to think of this as "what playbooks does this specific actor use"?
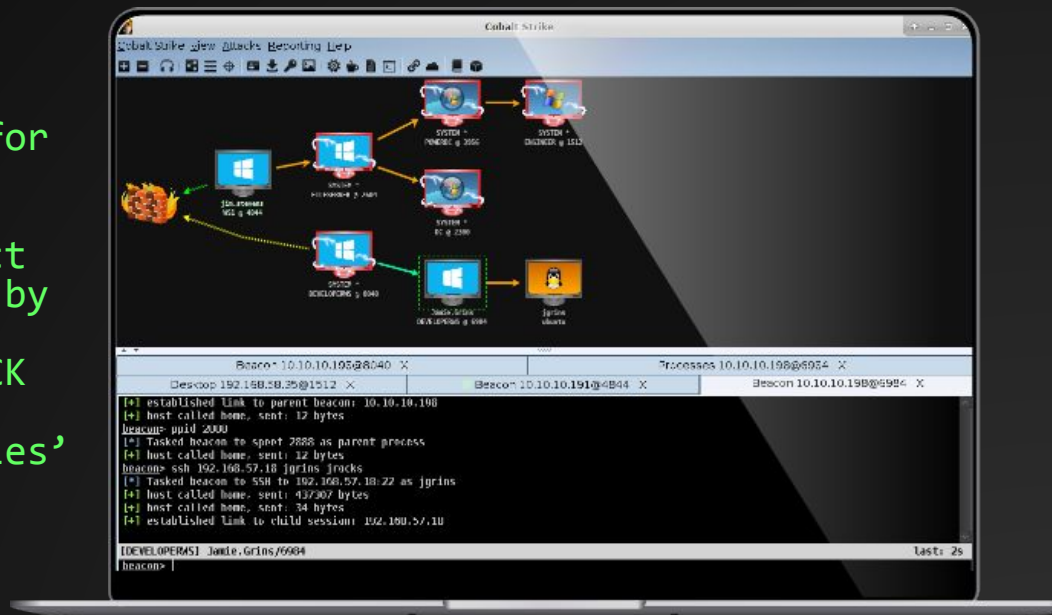
This course

- In this class, we will mostly use MITRE ATT&CK
- It is a valuable framework for comparing cyber operations
- In particular, lets look at the previous example comparing APT28 and APT29

Two separate Russian espionage groups

APT29

① Leverages → Operational Infrastructure

② Pushes → Implant

③ Establishes encrypted communication with → TARGETED SYSTEMS

④ Silently exfiltrates data

APT29 TRADECRAFT
• Powershell comand
• Scheduled execution
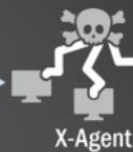• Unique encryption keys

TARGETED SYSTEMS

APT28
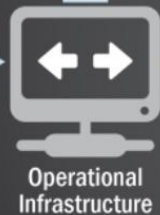
① Leverages → Operational Infrastructure

② Deploys → X-Agent

③ Installs onto

④ Leverages → X-Tunnel

⑤ Enables remote execution

APT28 TRADECRAFT
• Remote execution
• File transmission
• Keylogging

More Definitions

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)

Hash value: the unique fingerprint of a single file

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

Domain Name: an entry for a A/AAAA record used by a DNS servers to map human friendly names (like google.com) to computer friendly IP addresses (8.8.8.8).
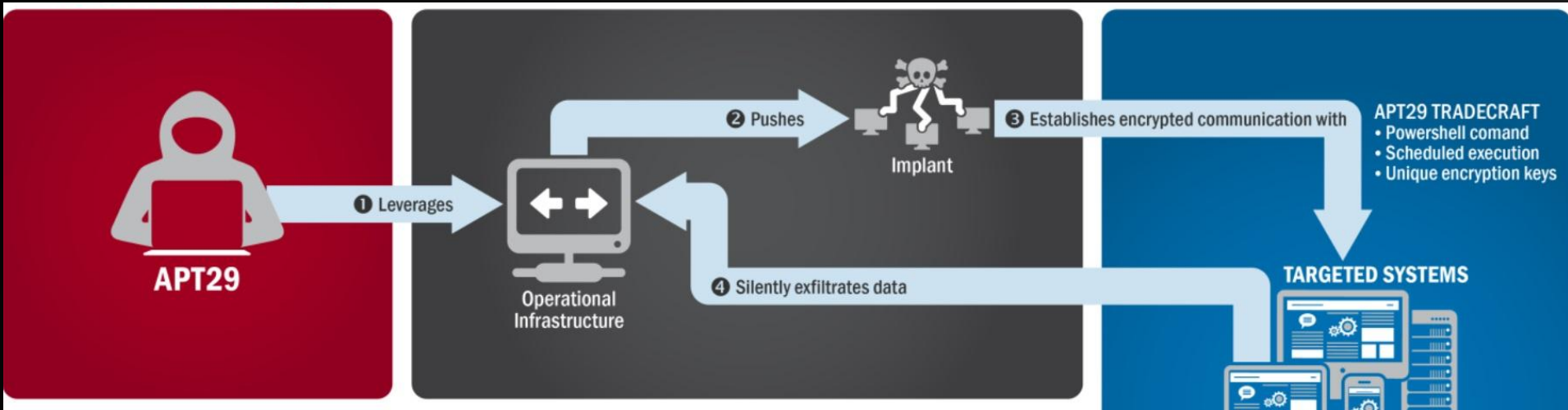
Blue team: how do I make sure this attacker can't successfully compromise our network?

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

Life of a Blue Teamer/ SOC analyst

- Find Indicators of Compromise
- Move from Indicators of Compromise (IOCs) to -> Tactics, techniques and procedures (TTPs)
- Protecting your Environment from the Tactics / Techniques/ Procedures used.
- Break Links in the "cyber killchain"
- Eventually, threats evolve to combat your countermeasures. Go back to step 1 :)

Threat Analysis Pyramid of Pain
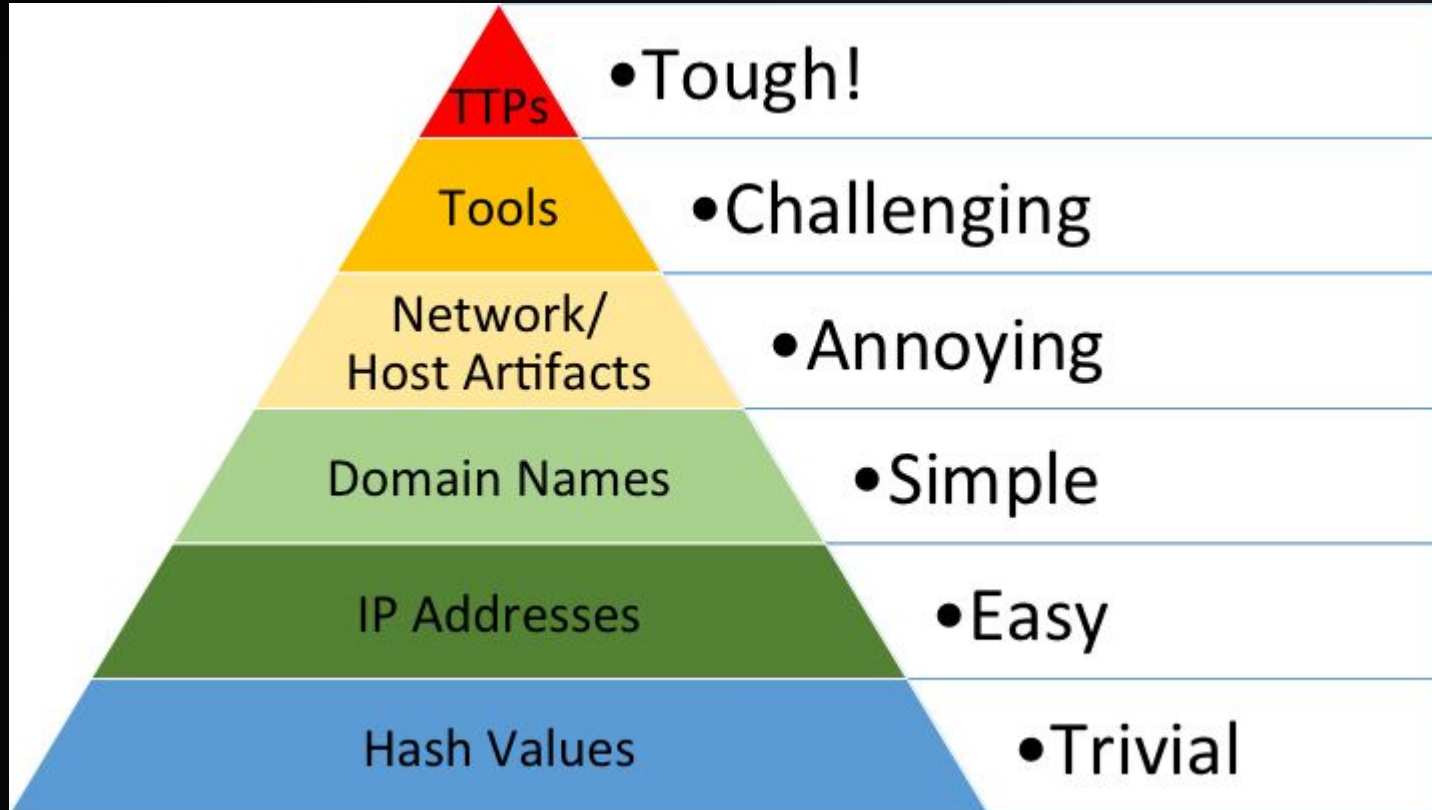
Threat Analysis Pyramid of Pain
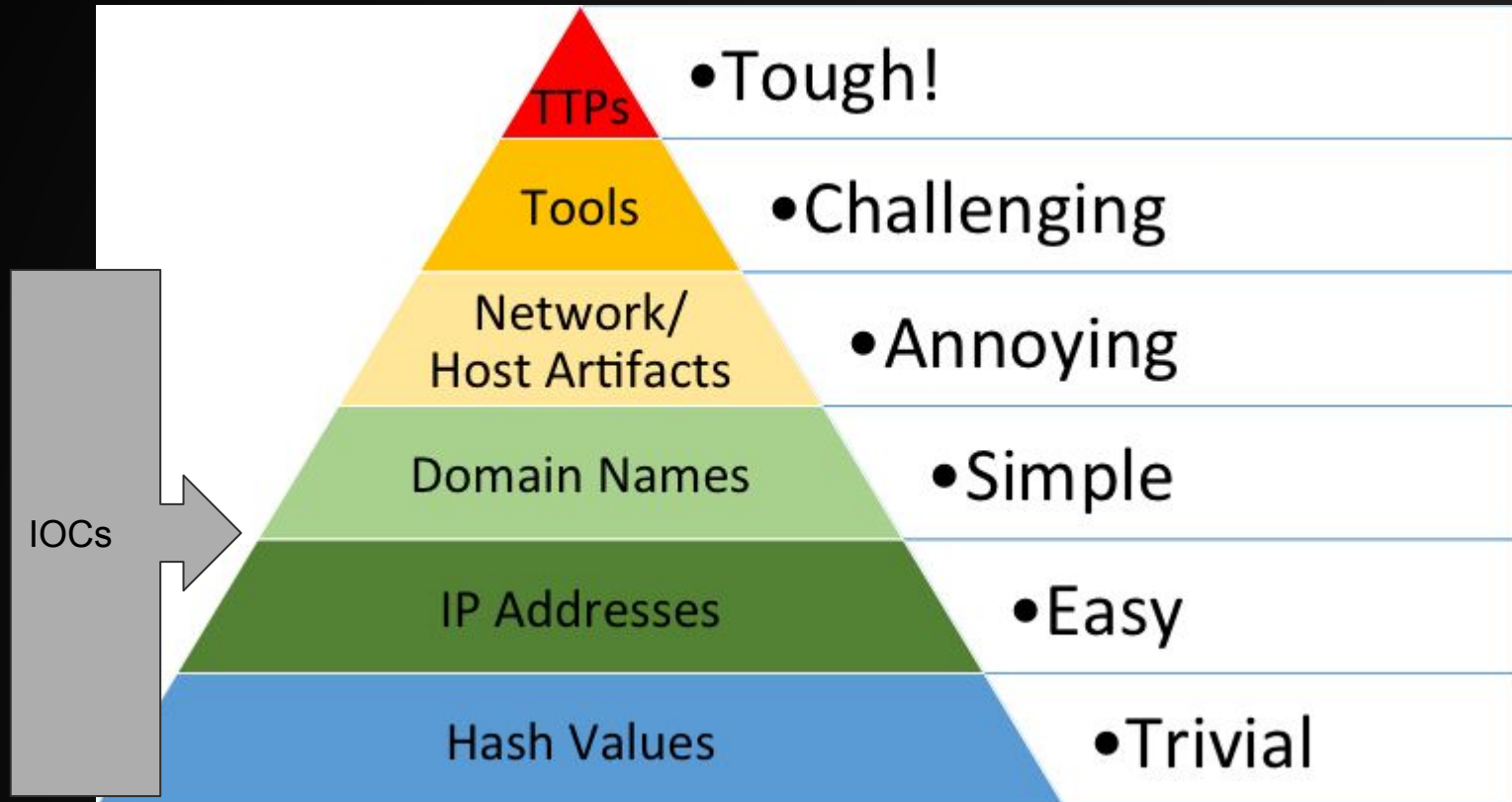
Threat Analysis Pyramid of Pain

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?
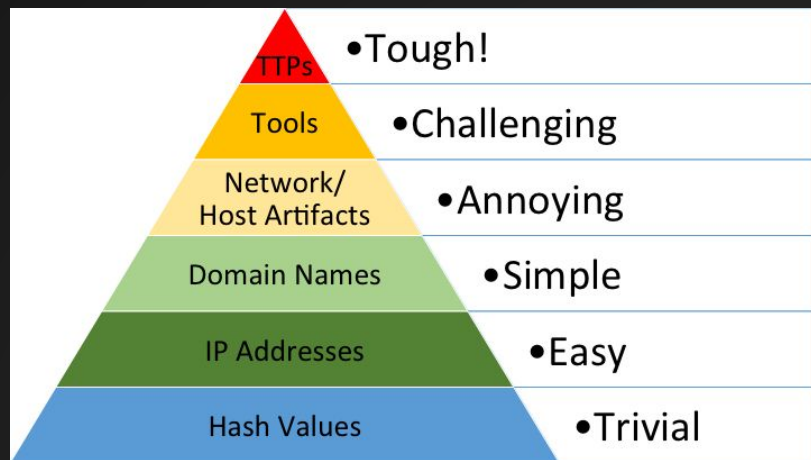
Easy…until it isn't!

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.

Or…you know what if someone compromises a bunch of legitimate sites and use them to carry out cyber operation?
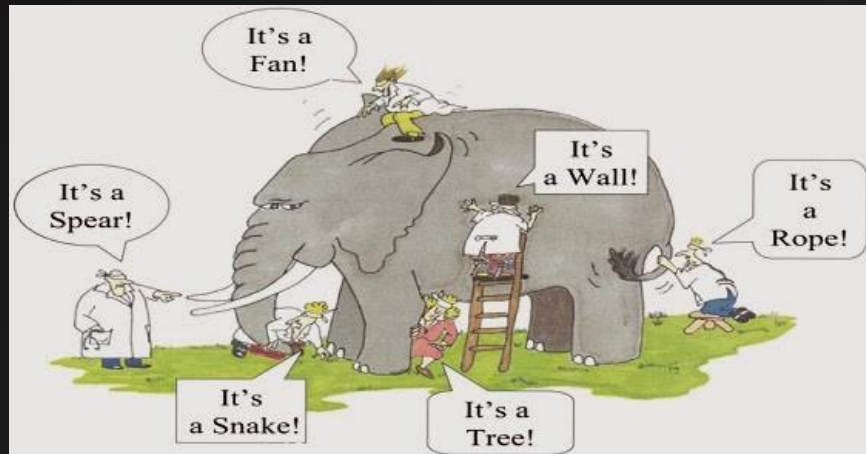
Different companies see different IOCs

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.

Reminder!
Different entities also use
different jargon!

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, and imports!

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

Discussion:
What do we need to control a computer?