
Cyber attackers
CalPolyPomona

Cyber attackers: classification attributes

- **Internal vs. External:** We most often think about the threat actors who exist outside our organizations: competitors, criminals, and the curious. However, some of the most dangerous threats come from within our own environments.
  - Complex attacks often come from externals with some internal complicity
- **Level of Sophistication/Capability:** Threat actors vary greatly in their level of cybersecurity sophistication and capability. As we explore different types of threat actors in this lesson, we'll discuss how they range from the unsophisticated *script kiddie* simply running code borrowed from others to the *advanced persistent threat* (APT) actor exploiting vulnerabilities discovered in their own research labs and unknown to the security community.
- **Resources/Funding:** Just as threat actors vary in their sophistication, they also vary in the resources available to them. Highly organized attackers sponsored by criminal syndicates or national governments often have virtually limitless resources, whereas less organized attackers may simply be hobbyists working in their spare time.
- **Intent/Motivation:** Attackers also vary in their motivation and intent. The *script kiddie* may be simply out for the thrill of the attack, whereas competitors may be engaged in highly targeted corporate espionage. *Nation-states* seek to achieve political objectives; criminal syndicates often focus on direct financial gain.

The Hats Hackers Wear

The cybersecurity community uses a shorthand lingo to refer to the motivations of attackers, describing them as having different-colored hats. The origins of this approach date back to old Western films, where the “good guys” wore white hats, and the “bad guys” wore black hats to help distinguish them in the film. Cybersecurity professionals have adopted this approach to describe different types of cybersecurity adversaries:

- **White-hat hackers,** also known as authorized attackers, are those who act with authorization and seek to discover security vulnerabilities with the intent of correcting them. White-hat attackers may either be employees of the organization or contractors hired to engage in ***penetration testing*** (they are often called ***penetration testers***).
- **Black-hat hackers**, also known as unauthorized attackers, are those with malicious intent. They seek to defeat security controls and compromise the confidentiality, integrity, or availability of information and systems for their own, unauthorized, purposes.
- **Gray-hat hackers**, also known as semi-authorized attackers, are those who fall somewhere between white- and black-hat hackers. They act without proper authorization, but they do so with the intent of informing their targets of any security vulnerabilities. It's important to understand that simply having good intent does not make gray-hat hacking legal or ethical. The techniques used by gray-hat attackers can still be punished as criminal offenses.

Classes of Intruders: *Cyber Criminals*

- Individuals or members of an organized crime group with a goal of financial reward
- Their activities may include:
  - Identity theft: stealing and using information and documents by someone else with a false identity. E.g., opening accounts, posting on social media, performing transactions, accessing physically secured areas
  - Theft of financial credentials: stealing of data for financial purposes
  - Corporate espionage: stealing information for accessing business or secreted information. E.g., inventions and patents, political secrets
  - Data theft: generic stealing of data for different purposes: e.g., copyright violation, re-sale, etc.
  - Data ransoming: "kidnapping" data to be released after payment
- Typically, they are young who do business on the Web
- They meet in underground forums to trade tips and data and coordinate attacks

One of the key threats to security is the use of some form of hacking by an intruder, often referred to as a hacker or cracker. Verizon [VERI16] indicates that 92% of the breaches they investigated were by outsiders, with 14% by insiders, and with some breaches involving both outsiders and insiders. They also noted that insiders were responsible for a small number of very large dataset compromises. Both Symantec [SYMA16] and Verizon [VERI16] also comment that not only is there a general increase in malicious hacking activity, but also an increase in attacks specifically targeted at individuals in organizations and the IT systems they use. This trend emphasizes the need to use defense-in-depth strategies, since such targeted attacks may be designed to bypass perimeter defenses such as firewalls and network-based Intrusion detection systems (IDSs).

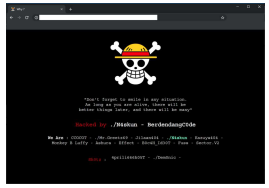
As with any defense strategy, an understanding of possible motivations of the attackers can assist in designing a suitable defensive strategy. Again, both Symantec [SYMA16] and Verizon [VERI16] comment on the following broad classes of intruders:

• **Cyber criminals**: Are either individuals or members of an organized crime group with a goal of financial

reward. To achieve this, their activities may include identity theft, theft of financial credentials, corporate espionage, data theft, or data ransoming. Typically, they are young, who do business on the Web [ANTE06]. They meet in underground forums with names like DarkMarket.org and theftservices.com to trade tips and data and coordinate attacks. For some years reports such as [SYMA16] have quoted very large and increasing costs resulting from cyber-crime activities, and hence the need to take steps to mitigate this threat.

Classes of Intruders: *Activists/Hacktivist*

- Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes
- Also know as hacktivists
  - Skill level is often quite low
- Aim of their attacks is often to promote and publicize their cause typically through:
  - Website defacement: partial or total alternation of victim website
  - Denial of Service attacks: interruption of service from victim of attack
  - Reputation: Theft and distribution of data that results in negative publicity or compromise of their targets
- Examples: Anonymous, Edward Snowden, etc.



CalPolyPomona | 5 Formicola

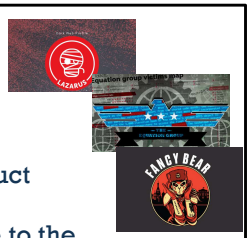
• **Activists**: Are either individuals, usually working as insiders, or members of a larger group of outsider attackers, who are motivated by social or political causes. They are also known as hacktivists, and their skill level is often quite low. The aim of their attacks is often to promote and publicize their cause, typically through website defacement, denial of service attacks, or the theft and distribution of data that results in negative publicity or compromise of their targets. Well-known recent examples include the activities of the groups Anonymous and LulzSec, and the actions of Chelsea (born Bradley) Manning and Edward Snowden.

Hacktivists use hacking techniques to accomplish some activist goal. They might deface the website of a company whose policies they disagree with. Or a hacktivist might attack a network due to some political issue. The defining characteristic of hacktivists is that they believe they are motivated by the greater good, even if their activity violates the law. Their activist motivation means that measures that might deter other attackers will be less likely to deter a hacktivist. Because they believe that they are engaged in a just crusade, they will, at least in some instances, risk getting caught to accomplish their goals. They may even view being caught as a badge of honor and a sacrifice for their cause. The skill levels of hacktivists vary widely. Some are only script kiddies, whereas others are quite skilled, having honed their craft over the years. In fact, some cybersecurity

researchers believe that some hacktivists are actually employed as cybersecurity professionals as their “day job” and perform hacktivist attacks in their spare time. Highly skilled hacktivists pose a significant danger to their targets. The resources of hacktivists also vary somewhat. Many are working alone and have very limited resources. However, some are part of organized efforts. The hacking group Anonymous is the most well-known hacktivist group. They collectively decide their agenda and their targets. Over the years, Anonymous has waged cyberattacks against targets as diverse as the Church of Scientology, PayPal, Visa and Mastercard, Westboro Baptist Church, and even government agencies.

This type of anonymous collective of attackers can prove quite powerful. Large groups will always have more time and other resources than a lone attacker. Due to their distributed and anonymous nature, it is difficult to identify, investigate, and prosecute participants in their hacking activities. The group lacks a hierarchical structure, and the capture of one member is unlikely to compromise the identities of other members. Hacktivists tend to be external attackers, but in some cases, internal employees who disagree strongly with their company's policies engage in hacktivism. In those instances, it is more likely that the hacktivist will attack the company by releasing confidential information. Government employees and self-styled whistleblowers fit this pattern of activity, seeking to bring what they consider unethical government actions to the attention of the public. For example, many people consider Edward Snowden a hacktivist. In 2013, Snowden, a former contractor with the U.S. National Security Agency, shared a large cache of sensitive government documents with journalists. Snowden's actions provided unprecedented insight into the digital intelligence gathering capabilities of the United States and its allies.

Classes of Intruders: *State-Sponsored Organizations*



- Groups of hackers sponsored by governments to conduct espionage or sabotage activities
- Also known as Advanced Persistent Threats (APTs) due to the covert nature and persistence over extended periods involved with any attacks in this class
- Widespread nature and scope of these activities by a wide range of countries:
  - E.g,. from one country against another

Not all but some of the groups indicated here https://attack.mitre.org/groups/ are *state-sponsored*

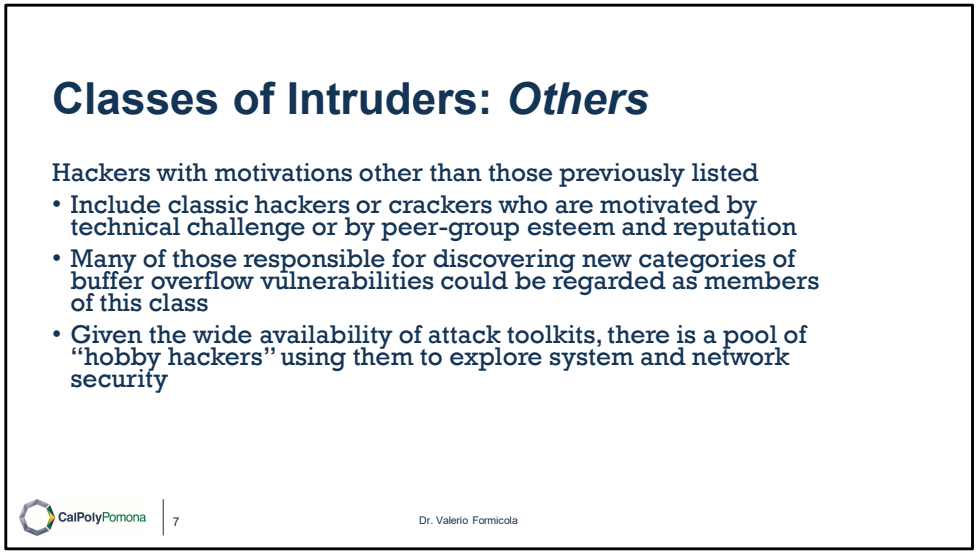
CalPolyPomona | 6 Dr. Valerio Formicola

• **State-sponsored organizations**: Are groups of hackers sponsored by governments to conduct espionage or sabotage activities. They are also known as Advanced Persistent Threats (APTs), due to the covert nature and persistence over extended periods involved with many attacks in this class. Recent reports such as [MAND13], and information revealed by Edward Snowden, indicate the widespread nature and scope of these activities by a wide range of countries from China to the USA, UK, and their intelligence allies.

Groups are activity clusters that are tracked by a common name in the security community. Analysts track these clusters using various analytic methodologies and terms such as threat groups, activity groups, and threat actors. Some groups have multiple names associated with similar activities due to various organizations tracking similar activities by different names. Organizations' group definitions may partially overlap with groups designated by other organizations and may disagree on specific activity.
For the purposes of the Group pages, the MITRE ATT&CK team uses the term Group to refer to any of the above designations for an adversary activity cluster. The team makes a best effort to track overlaps between names based on publicly reported associations, which are designated as “Associated Groups” on each page (formerly labeled “Aliases”), because we believe these overlaps are useful for analyst awareness. We do not

represent these names as exact overlaps and encourage analysts to do additional research.
Groups are mapped to publicly reported technique use and original references are included. The information provided does not represent all possible technique use by Groups, but rather a subset that is available solely through open source reporting. Groups are also mapped to reported Software used and attributed Campaigns, and related techniques for each are tracked separately on their respective pages.

https://www.varonis.com/blog/apt-groups

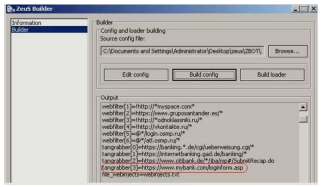


• **Others**: Are hackers with motivations other than those listed above, including classic hackers or crackers who are motivated by technical challenge or by peer-group esteem and reputation. Many of those responsible for discovering new categories of buffer overflow vulnerabilities [MEER10] could be regarded as members of this class. Also, given the wide availability of attack toolkits, there is a pool of "hobby hackers" using them to explore system and network security, who could potentially become recruits for the above classes

Intruder Skill Levels – Apprentice/Beginner

- Hackers with minimal technical skill who primarily use existing **attack toolkits** (aka, **crimeware**)
  - E.g. Zeus toolkit, Angler
- They likely comprise the largest number of attackers, including many criminal and activist attackers
- Also known as "**script-kiddies**" due to their use of existing scripts (tools)

Given their use of existing known tools, these attackers are the easiest to defend against



https://www.pdf-archive.com/2011/03/26/zeus-crimeware-toolkit/

CalPolyPomona | 8 Dr. Valerio Formicola

Across these classes of intruders, there is also a range of skill levels seen. These can be broadly classified as:

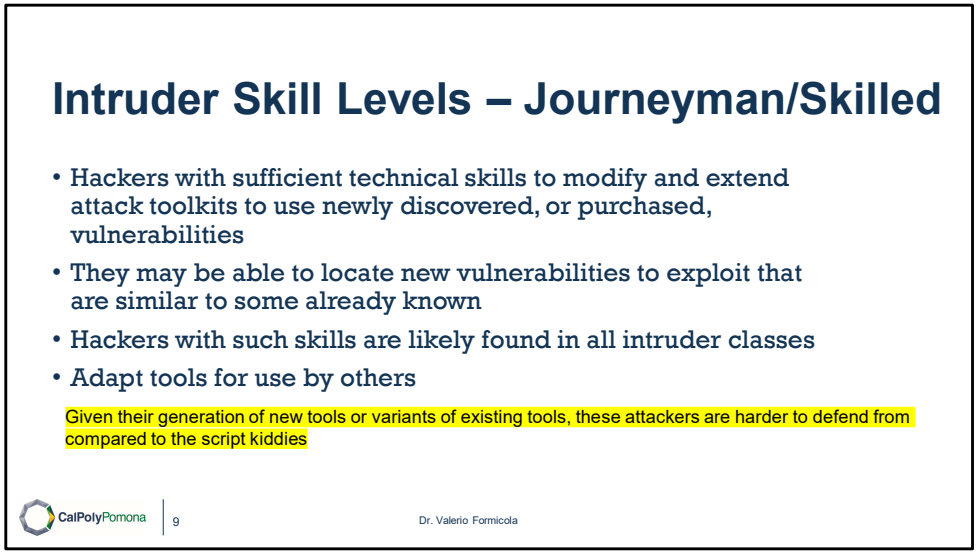
• **Apprentice**: Hackers with minimal technical skill who primarily use existing attack toolkits. They likely comprise the largest number of attackers, including many criminal and activist attackers. Given their use of existing known tools, these attackers are the easiest to defend against. They are also known as "script-kiddies" due to their use of existing scripts (tools).

The term script kiddie is a derogatory term for people who use hacking techniques but have limited skills. Often such attackers may rely almost entirely on automated tools they download from the Internet. These attackers often have little knowledge of how their attacks actually work, and they are simply seeking out convenient targets of opportunity. You might think that with their relatively low skill level, script kiddies are not a real security threat. However, that isn't the case for two important reasons. First, simplistic hacking tools are freely available on the Internet. If you're vulnerable to them, anyone can easily find tools to automate denial-of-service (DoS) attacks, create viruses, make a Trojan horse, or even distribute ransomware as a service. Personal technical skills are no longer a barrier to attacking a network. Second, script kiddies are plentiful and unfocused in their work. Although the nature of your business might not find you in the

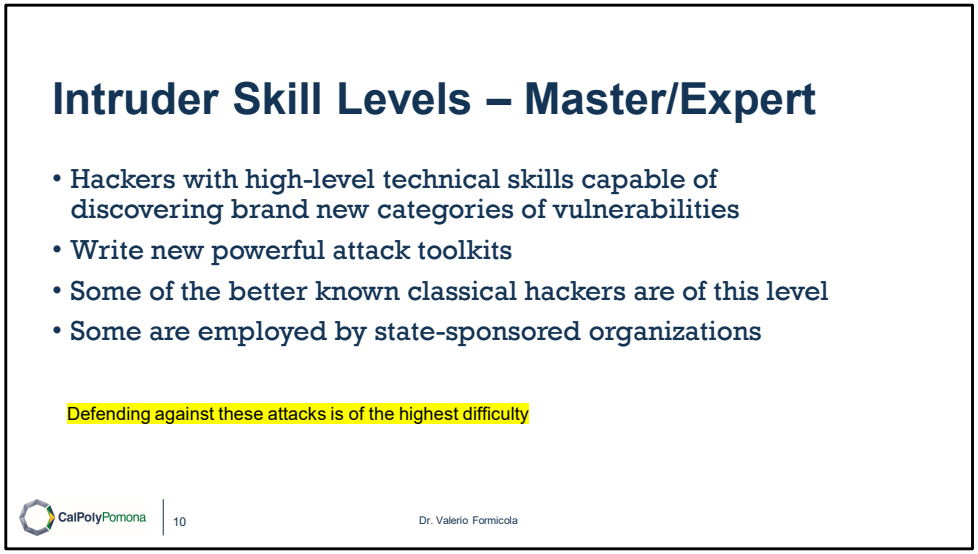
crosshairs of a sophisticated military-sponsored attack, script kiddies are much less discriminating in their target selection. They often just search for and discover vulnerable victims without even knowing the identity of their target. They might root around in files and systems and only discover who they've penetrated after their attack succeeds. In general, the motivations of script kiddies revolve around trying to prove their skill. In other words, they may attack your network simply because it is there. Secondary school and university networks are common targets of script kiddies attacks because many of these attackers are school-aged individuals. Fortunately, the number of script kiddies is often offset by their lack of skill and lack of resources. These individuals tend to be rather young, they work alone, and they have very few resources. And by resources, we mean time as well as money. A script kiddie normally can't attack your network 24 hours a day. They usually have to work a job, go to school, and attend to other life functions.

Initially, the development and deployment of malware required considerable technical skill by software authors. This changed with the development of virus- creation toolkits in the early 1990s, and then later of more general attack kits in the 2000s, that greatly assisted in the development and deployment of malware [FOSS10]. These toolkits, often known as **crimeware**, now include a variety of propagation mechanisms and payload modules that even novices can combine, select, and deploy. They can also easily be customized with the latest discovered vulnerabilities in order to exploit the window of opportunity between the publication of a weakness and the widespread deployment of patches to close it. These kits greatly enlarged the population of attackers able to deploy malware. Although the malware created with such toolkits tends to be less sophisticated than that designed from scratch, the sheer number of new variants that can be generated by attackers using these toolkits creates a significant problem for those defending systems against them.

The Zeus crimeware toolkit is a prominent example of such an attack kit, which was used to generate a wide range of very effective, stealthed malware that facilitates a range of criminal activities, in particular capturing and exploiting banking credentials [BINS10]. The Angler exploit kit, first seen in 2013, was the most active kit seen in 2015, often distributed via malvertising that exploited Flash vulnerabilities. It is sophisticated and technically advanced, in both attacks executed and counter-measures deployed to resist detection. There are a number of other attack kits in active use, though the specific kits change from year to year as attackers continue to evolve and improve them [SYMA16].



• **Journeyman**: Hackers with sufficient technical skills to modify and extend attack toolkits to use newly discovered, or purchased, vulnerabilities; or to focus on different target groups. They may also be able to locate new vulnerabilities to exploit that are similar to some already known. A number of hackers with such skills are likely found in all intruder classes listed above, adapting tools for use by others. The changes in attack tools make identifying and defending against such attacks harder.



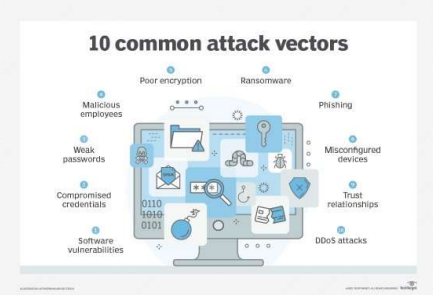
Hackers with high-level technical skills capable of discovering brand new categories of vulnerabilities, or writing new powerful attack toolkits. Some of the better-known classical hackers are of this level, as clearly are some of those employed by some state-sponsored organizations, as the designation APT suggests. This makes defending against these attacks of the highest difficulty.


Cyber attack stages
CalPolyPomona

Attack vectors

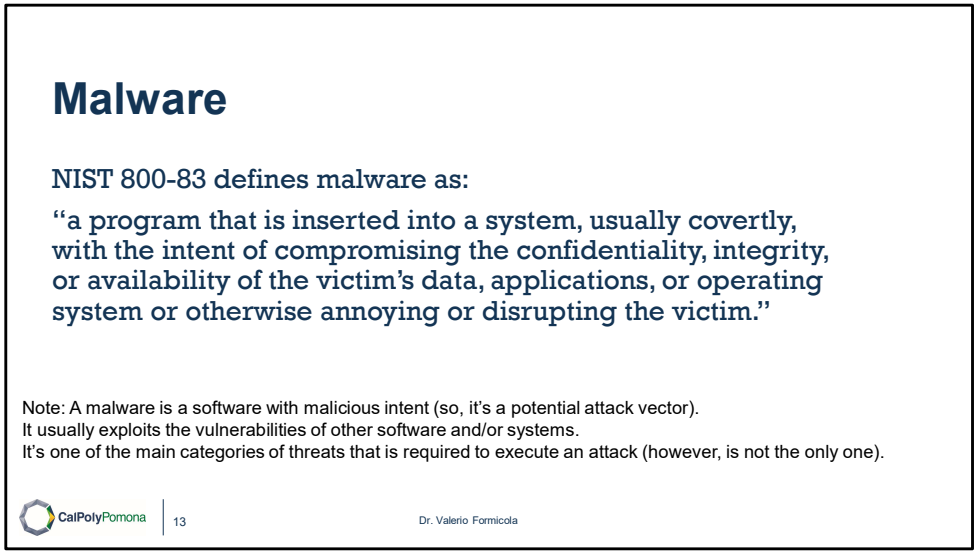
- An **attack vector** is a generic way to indicate the method or combination of methods that cybercriminals use to breach or infiltrate a victim's network.

- Adversaries typically develop an arsenal of attack vectors that they routinely use to carry out their attacks. Over time and with repeated use, these attack vectors can become virtual "calling cards" for cybercriminals or organized eCrime gangs, making it possible for threat intelligence analysts, cybersecurity service providers, law enforcement, and government agencies to assign an identity to different adversaries.
- Recognizing and tracking an adversary's attack vectors can help organizations better defend against existing or upcoming targeted attacks.



An attack vector is a very generic way to indicate the methods used to gain unauthorized access to a computer system or a network.

It includes Phyishing, Zero-day attacks, Social engineering attacks, Compromised and weak credentials, Insider threats, Security misconfiguration, Ransomware, Malware, Man-in-the-middle attacks (MITM), Session hijacking, Brute Force attacks, DDoS attacks



Malicious software, or **malware**, arguably constitutes one of the most significant categories of threats to computer systems. NIST SP 800-83 *(Guide to Malware Incident Prevention and Handling for Desktops and Laptops,* July 2013) defines malware as "a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim." Hence, we are concerned with the threat malware poses to application programs, to utility programs, such as editors and compilers, and to kernel-level programs. We are also concerned with its use on compromised or malicious Web sites and servers, or in especially crafted spam e-mails or other messages, which aim to trick users into revealing sensitive personal information.

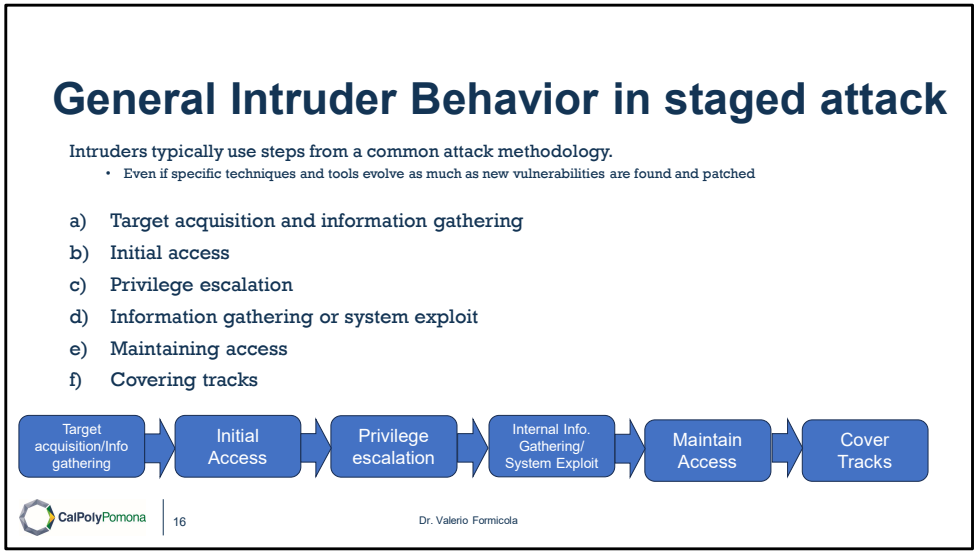
Table 6.1 Malware Terminology

Name	Description
Advanced Persistent Threat (APT)	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by-download	An attack using code on a compromised website that exploits a browser Vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.

The terminology in this area presents problems because of a lack of universal agreement on all of the terms and because some of the categories overlap. Table 6.1 is a useful guide to some of the terms in use.

Table 6.1 Malware Terminology (2 of 3)

Name	Description
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a Predefined condition is met; the code then triggers some payload.
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a Document or document template, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile code	Software (e.g., script and macro) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.



The techniques and behavior patterns of intruders are constantly shifting, to exploit newly discovered weaknesses and to evade detection and countermeasures. However, intruders typically use steps from a common attack methodology. [VERI16] in their "Wrap up" section illustrate a typical sequence of actions, starting with a phishing attack that results in the installation of malware that steals login credentials that eventually result in the compromise of a Point-of-Sale terminal. They note that while this is one specific incident scenario, the components are commonly seen in many attacks. [MCCL12] discuss in detail activities associated with the following steps:

- **Target Acquisition and Information Gathering**: Where the attacker identifies and characterizes the target systems using publicly available information, both technical and non-technical, and the use network exploration tools to map target resources.

- **Initial Access**: The initial access to a target system, typically by exploiting a remote network vulnerability as we discuss in Chapters 10 and 11, by guessing weak authentication credentials used in a remote service as we discussed in Chapter 3, or via the installation of malware on the system using some form of social

engineering or drive-by-download attack as we discuss in Chapter 6.

- **Privilege Escalation**: Actions taken on the system, typically via a local access vulnerability as discussed in Chapters 10 and 11, to increase the privileges available to the attacker to enable their desired goals on the target system.

- **Information Gathering or System Exploit:** Actions by the attacker to access or modify information or resources on the system, or to navigate to another target system.

- **Maintaining Access**: Actions such as the installation of backdoors or other malicious software as we discuss in Chapter 6, or through the addition of covert authentication credentials or other configuration changes to the system, to enable continued access by the attacker after the initial attack.

- **Covering Tracks:** Where the attacker disables or edits audit logs such as we discuss in Chapter 18, to remove evidence of attack activity, and uses rootkits and other measures to hide covertly installed files or code as we discuss in Chapter 6.

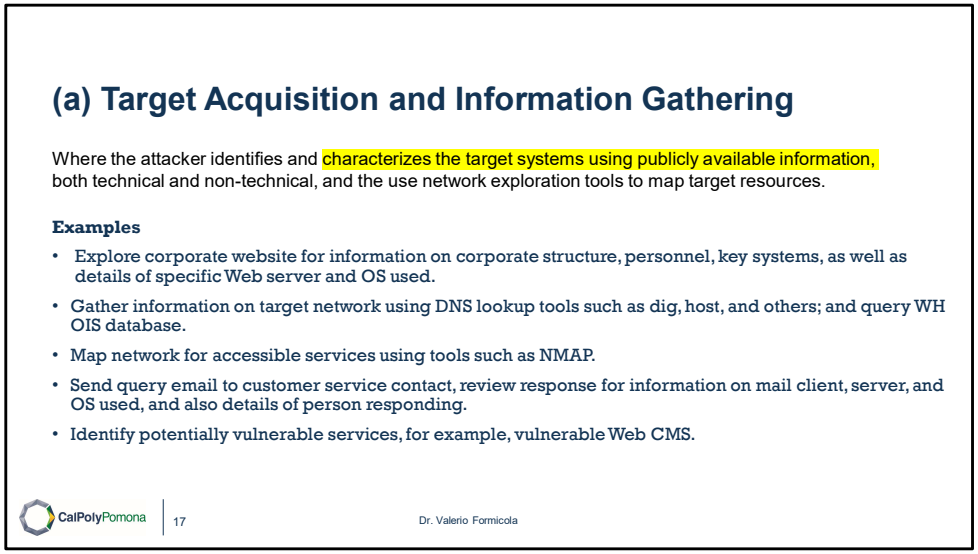


Table 8.1 lists examples of activities associated with the above steps.

(b) Initial Access

The initial access to a target system, typically by exploiting a remote network vulnerability, by guessing weak authentication credentials used in a remote service, or via the installation of malware on the system using some form of social engineering or drive-by-download.

Examples

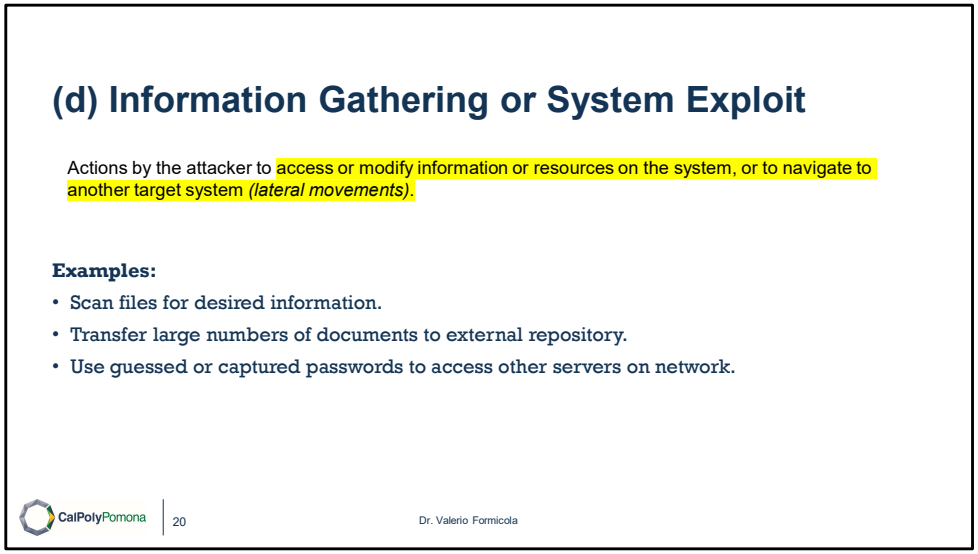
- Brute force (guess) a user's Web content management system (CMS) password.
- Exploit vulnerability in Web CMS plugin to gain system access.
- Send spear-phishing e-mail with link to Web browser exploit to key people.

(c) Privilege Escalation

Actions taken on the system, typically via a local access vulnerability, to increase the privileges available to the attacker to enable their desired goals on the target system.

Examples

- Scan system for applications with local exploit.
- Exploit any vulnerable application to gain elevated privileges.
- Install sniffers to capture administrator passwords.
- Use captured administrator password to access privileged information.



Lateral movement refers to **the techniques that a cyberattacker uses, after gaining initial access, to move deeper into a network** in search of sensitive data and other high-value assets. After entering the network, the attacker maintains ongoing access by moving through the compromised environment and obtaining increased privileges using various tools.

(e) Maintaining Access

Actions such as the installation of backdoors or other malicious software, or through the addition of covert authentication credentials or other configuration changes to the system, to enable continued access by the attacker after the initial attack.

Examples:

- Install remote administration tool or rootkit with backdoor for later access.
- Use administrator password to later access network.
- Modify or disable anti-virus or IDS programs running on system.

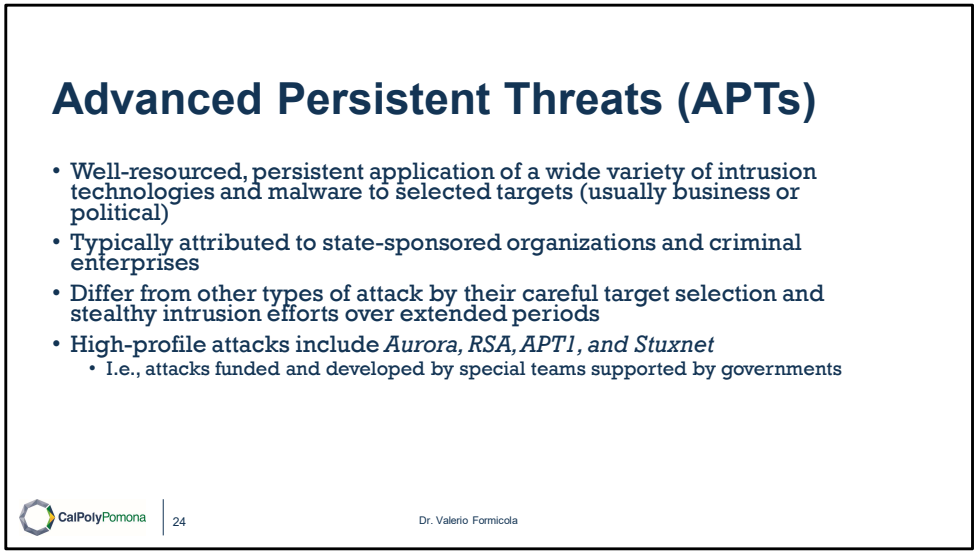
(f) Covering Tracks

Where the attacker disables or edits audit logs, to remove evidence of attack activity, and uses rootkits and other measures to hide covertly installed files or code.

Examples

- Use rootkit to hide files installed on system.
- Edit logfiles to remove entries generated during the intrusion.


Advanced Persistent Threats (APT) and models
CalPolyPomona



In recent years, a great deal of attention has been given to state actors hacking into either foreign governments or corporations. The security company Mandiant created the term advanced persistent threats (APTs) to describe a series of attacks that they first traced to sources connected to the Chinese military. In subsequent years, the security community discovered similar organizations linked to the government of virtually every technologically advanced country. The term APT tells you a great deal about the attacks themselves. First, they used advanced techniques, not simply tools downloaded from the Internet. Second, the attacks are persistent, occurring over a significant period of time. In some cases, the attacks continued for years as attackers patiently stalked their targets, awaiting the right opportunity to strike. The APT attacks that Mandiant reported are emblematic of nation-state attacks. They tend to be characterized by highly skilled attackers with significant resources. A nation has the labor force, time, and money to finance ongoing, sophisticated attacks. The motive can be political or economic. In some cases, the attack is done for traditional espionage goals: to gather information about the target's defense capabilities. In other cases, the attack might be targeting intellectual property or other economic assets.

A number of high-profile attacks, including Aurora, RSA, APT1, and Stuxnet, are often cited as examples.

APT Characteristics (1 of 2)

- **Advanced**
  - Used by the attackers of a **wide variety of intrusion technologies and** malware including the development of **custom malware** if required
    - For example, Zero day exploits, social engineering, phishing
  - The individual components may not necessarily be technically advanced but a carefully selected to **suit the chosen target**

- **Persistent**
  - Determined application of the attacks over an **extended period** against the chosen target in order to maximize the chance of success
  - A variety of **attacks may be progressively applied** until the target is compromised

CalPolyPomona | 25 | Dr. Valerio Formicola

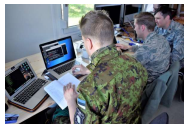
They are named as a result of these characteristics:

• **Advanced**: Use by the attackers of a wide variety of intrusion technologies and malware, including the development of custom malware if required. The individual components may not necessarily be technically advanced, but are carefully selected to suit the chosen target.

• **Persistent:** Determined application of the attacks over an extended period against the chosen target in order to maximize the chance of success. A variety of attacks may be progressively, and often stealthily, applied until the target is compromised.

• **Threats**: Threats to the selected targets as a result of the organized, capable, and well-funded attackers intent to compromise the specifically chosen targets. The active involvement of people in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attack.

APT Characteristics (2 of 2)



- **Threats**
  - Threats to the selected targets as a result of the **organized, capable, and well-funded attackers** intent **to compromise** the specifically **chosen targets**
  - The **active involvement of people** in the process greatly raises the threat level from that due to automated attacks tools, and also the likelihood of successful attacks
    - I.e., many experts of specific target systems and devices are involved in the creation of malwares and attack strategies.
    - For example, experts of specific software installed inside a commercial industrial control system, electric system, power plant, machine, etc.

E.g., APT against banks: https://www.banktech.com/anatomy-of-an-advanced-persistent-threat-attack/a/d-id/1316528.html

APT and Zero-day exploits

- **APT make large use of Zero-day exploits**
- APT attackers often conduct their own security vulnerability research in an attempt to discover vulnerabilities that are not known to other attackers or cybersecurity teams.
- After they uncover a vulnerability, they do not disclose it but rather store it in a vulnerability repository for later use.
- Zero-day attacks are particularly dangerous because they are unknown to product vendors, and therefore, no patches are available to correct them. APT actors who exploit zero-day vulnerabilities are often able to easily compromise their targets.
  - Stuxnet is one of the most well-known examples of an APT attack. The Stuxnet attack, traced to the U.S. and Israeli governments, exploited zero-day vulnerabilities to compromise the control networks at an Iranian uranium enrichment facility.

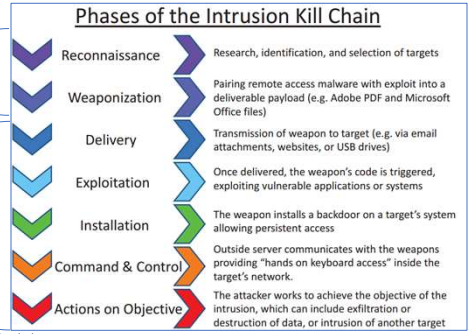
https://attack.mitre.org/groups/

Staged cyber attacks models: Cyber Kill Chain by Lockheed Martin

- In 2011, Lockheed Martin published Cyber Kill Chain as one of the first attempts to explain how APT attacks work. The Cyber Kill Chain covers 7 high level goals, or tactics, attackers perform during an attack. As one can see from the original publication, these 7 steps are very easy to understand and communicate

PRE-ATTACK STAGES

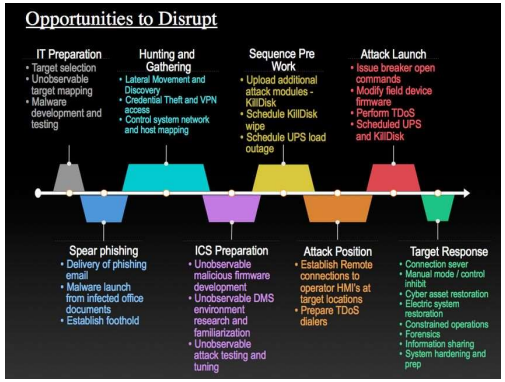
ATTACK STAGES



Problems is the Cyber Kill Chain covers only high-level tactics (goals or phases) of an attack. This framework is great for speaking to non-practitioners about a particular attack, how it occurred, and maybe even discussing how the cyber kill chain can be broken by defenders before the attackers are successful.

Example: Attack to the Ukraine power grid in 2015 (SANS report)

On December 23, 2015, the power grid in two western oblasts of Ukraine was hacked, which resulted in power outages for roughly 230,000 consumers in Ukraine for 1-6 hours. The attack took place during the ongoing Russo-Ukrainian War (2014-present) and is attributed to a Russian advanced persistent threat group known as "Sandworm". It is the first publicly acknowledged successful cyberattack on a power grid.



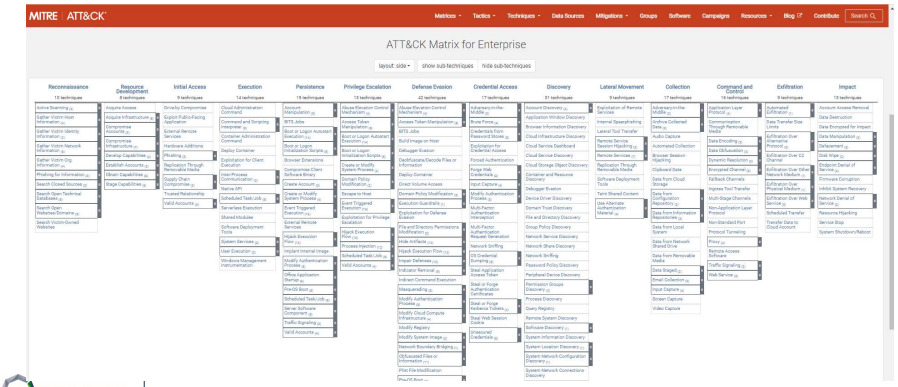
https://icscsi.org/library/Documents/Cyber_Events/E-ISAC%20-%20Analysis%20of%20the%20Cyber%20Attack%20on%20the%20Ukrainian%20Power%20Grid.pdf

Cyber Kill Chain model - MITRE ATT&CK

- In 2015, MITRE released ATT&CK: Adversary Tactics, Techniques, and Common Knowledge. This is the current industry standard and most used framework for understanding and communicating how attacks work. It goes a step further than the Cyber Kill Chain by expanding the attackers' high-level goals to 14 different tactics.

https://doc.sophos.com/central/mdr/help/en-us/welcomeguides/mdr/index.html

MITRE ATT&CK framework (enterprise - map view)



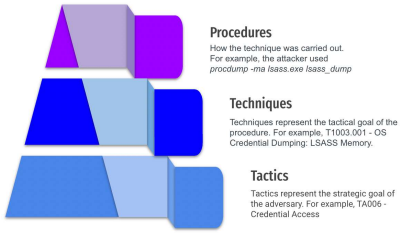
Dr. Valerio Formicola

https://attack.mitre.org/

Tactics, Techniques, and Procedures (TTP)

Tactics, Techniques, and Procedures (TTP) is the method used by IT and military professionals to determine the behavior of a threat actor (hacker). These three elements help you understand your adversaries better.

- **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.
- **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.
  - **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.
- **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.

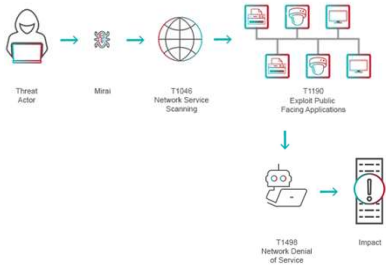


While each element is important by itself, by studying all three elements, attacks can more easily be hunted down, identified, and neutralized. Knowing a hacker's TTP's can help you identify attacks early enabling you to neutralize them before significant damage is done.

https://attack.mitre.org/resources/faq/

Example of TTP from a kill chain

- **Mirai** is a piece of malware that turns IoT devices (e.g., Internet cameras) running the Linux operating system into controlled 'bots' that can be used as part of a botnet in large-scale network DDoS attacks.



Check the TTP IDs on Mitre

Impact	Technique	ID	Description
Initial Access	Exploit Public-Facing Applications	T1190	Mirai variants take advantage of design vulnerabilities in internet facing IoT devices by exploiting SSH/Telnet
Lateral Movement	Exploitation of Remote Services	T1210	Mirai variants spread through remote code execution (RCE) vulnerabilities
Discovery	Network Service Scanning	T1046	Mirai conducts internet wide scans to discover new vulnerable IoT devices
Credential Access	Brute Force	T1110	Mirai leverages a list of hardcoded credentials to brute force IoT devices through Telnet and SSH
Execution	Exploitation for Client Execution	T1203	Demonbot was observed attempting to exploit known vulnerabilities in Hadoop
Command and Control	Domain Generation Algorithms	T1520	A Mirai variant was observed using DGA for protecting its command and control infrastructure
Defense Evasion	Connection Proxy	T1090	Botnets such as OMG, VPNFilter create anonymizing proxy networks through socks enabled bots leveraging open source software such as 3proxy. UPnP vulnerabilities in consumer routers have been abused to create port forwarding schemes that conceal malicious communications and attacks through port-hopping across multiple routers
Impact	Network Denial of Service	T1498	Mirai can conduct network denial-of-service attacks
Impact	Endpoint Denial of Service	T1499	Mirai can conduct endpoint denial-of-service attacks such as simple HTTP(S) floods

https://www.radware.com/security/ddos-experts-insider/hackers-corner/tactics-techniques-procedures/

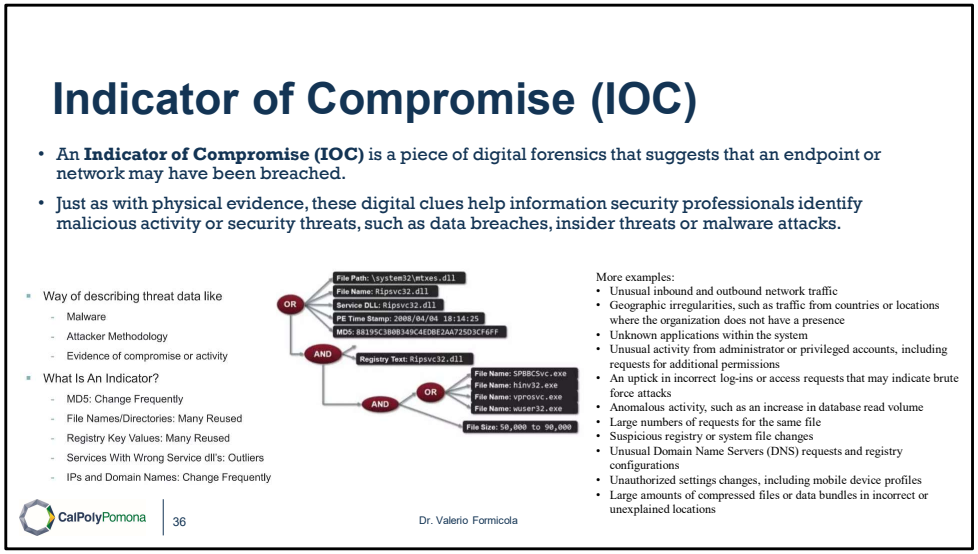
Unified Kill Chain model

In 2017, Paul Pols published the Unified Cyber Kill Chain to overcome and expand on the Cyber Kill Chain of Lockheed Martin and MITRE. (This is an Academic attempt to model attacks rather than purely technical)

The Unified Kill Chain			
1	**Reconnaissance**	Researching, identifying and selecting targets using active or passive reconnaissance.	*In* stage or *Initial Foothold*
2	**Weaponization**	Preparatory activities aimed at setting up the infrastructure required for the attack.	
3	**Delivery**	Techniques resulting in the transmission of a weaponized object to the targeted environment.	
4	**Social Engineering**	Techniques aimed at the manipulation of people to perform unsafe actions.	
5	**Exploitation**	Techniques to exploit vulnerabilities in systems that may, amongst others, result in code execution.	
6	**Persistence**	Any access, action or change to a system that gives an attacker persistent presence on the system.	
7	**Defense Evasion**	Techniques an attacker may specifically use for evading detection or avoiding other defenses.	
8	**Command & Control**	Techniques that allow attackers to communicate with controlled systems within a target network.	
9	**Pivoting**	Tunneling traffic through a controlled system to other systems that are not directly accessible.	*Through* stage or *Network Propagation*
10	**Discovery**	Techniques that allow an attacker to gain knowledge about a system and its network environment.	
11	**Privilege Escalation**	The result of techniques that provide an attacker with higher permissions on a system or network.	
12	**Execution**	Techniques that result in execution of attacker-controlled code on a local or remote system.	
13	**Credential Access**	Techniques resulting in the access of, or control over, system, service or domain credentials.	
14	**Lateral Movement**	Techniques that enable an adversary to horizontally access and control other remote systems.	
15	**Collection**	Techniques used to identify and gather data from a target network prior to exfiltration.	*Out* stage or *Action on Objectives*
16	**Exfiltration**	Techniques that result or aid in an attacker removing data from a target network.	
17	**Impact**	Techniques aimed at manipulating, interrupting or destroying the target system or data.	
18	**Objectives**	Socio-technical objectives of an attack that are intended to achieve a strategic goal.	

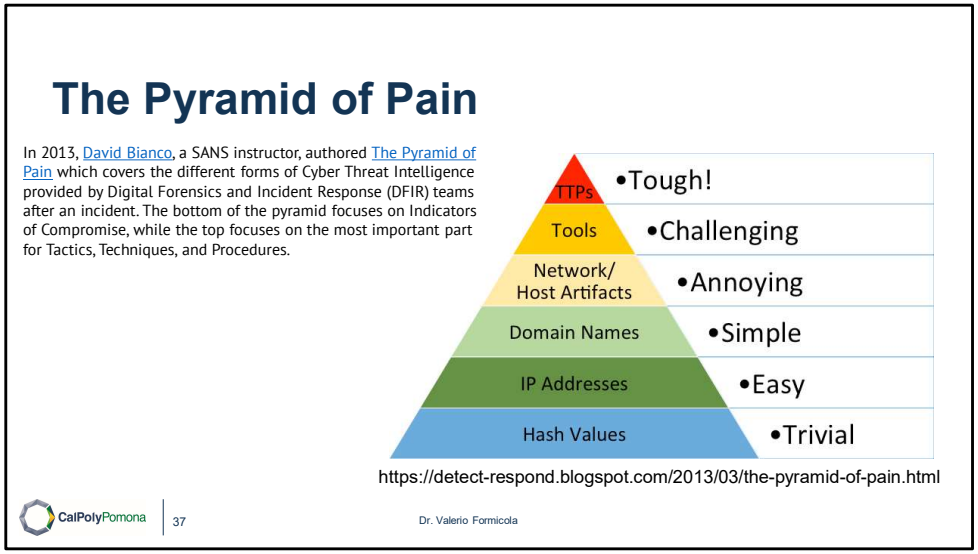
https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf


Digital forensics and
threat intelligence
CalPolyPomona



Digital forensics (sometimes known as **digital forensic science**) is a branch of forensic science encompassing the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computer crime.[1][2] The term "digital forensics" was originally used as a synonym for computer forensics but has expanded to cover investigation of all devices capable of storing digital data.

https://www.crowdstrike.com/cybersecurity-101/indicators-of-compromise/



Types of Indicators

Let's start by simply defining types of indicators make up the pyramid:

1.Hash Values: SHA1, MD5 or other similar hashes that correspond to specific suspicious or malicious files. Often used to provide unique references to specific samples of malware or to files involved in an intrusion.

2.IP Addresses: It's, um, an IP address. Or maybe a netblock.

3.Domain Names: This could be either a domain name itself (e.g., "evil.net") or maybe even a sub- or sub-sub-domain (e.g., "this.is.sooooo.evil.net")

4.Network Artifacts: Observables caused by adversary activities on your network. Technically speaking, every byte that flows over your network as a result of the adversary's interaction could be an artifact, but in practice this really means those pieces of the activity that might tend to distinguish malicious activity from that of legitimate users. Typical examples might be URI patterns, C2 information embedded in network protocols, distinctive HTTP User-Agent or SMTP Mailer values, etc.

5.Host Artifacts: Observables caused by adversary activities on one or more of your hosts. Again, we focus on things that would tend to distinguish malicious activities from legitimate ones. They could be registry

keys or values known to be created by specific pieces of malware, files or directories dropped in certain places or using certain names, names or descriptions or malicious services or almost anything else that's distinctive.

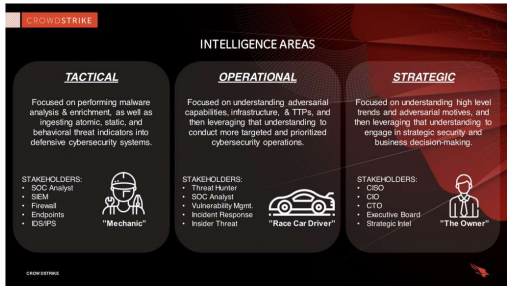
6. Tools: Software used by the adversary to accomplish their mission. Mostly this will be things they bring with them, rather than software or commands that may already be installed on the computer. This would include utilities designed to create malicious documents for spearphishing, backdoors used to establish C2 or password crackers or other host-based utilities they may want to use post-compromise.

7.Tactics, Techniques and Procedures (TTPs): How the adversary goes about accomplishing their mission, from reconnaissance all the way through data exfiltration and at every step in between. "Spearphishing" is a common TTP for establishing a presence in the network. "Spearphishing with a trojaned PDF file" or "... with a link to a malicious .SCR file disguised as a ZIP" would be more specific versions. "Dumping cached authentication credentials and reusing them in Pass-the-Hash attacks" would be a TTP. Notice we're not talking about specific tools here, as there are any number of ways of weaponizing a PDF or implementing Pass-the-Hash.

Cyber Threat Intelligence

Threat intelligence is evidence-based knowledge (e.g., context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets. – Gartner

1. **Tactical:** exchange/obtain **IOC** from feeds or internal intelligence. It's a very technical process of data collection about threats, to prepare/update defensive systems.
2. **Operational:** It gives insight into the origin and complexity of the group(s) involved and aids responders in comprehending the type, intent, and timeframe of a specific attack, hence, preventing next steps. (in other words, a Context for attack stages connected to APTs or known or unknown groups).
3. **Strategic:** It shows how global events, foreign policies, and other long-term local and international movements can potentially impact the cyber security of an organization.



Notes from https://heimdalsecurity.com/blog/operational-threat-intelligence/
and https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/

Tactical Threat intelligence (TTI) is focused on the immediate future, is technical in nature, and identifies simple indicators of compromise (IOCs). IOCs are things such as bad IP addresses, URLs, file hashes and known malicious domain names. It can be machine-readable, which means that security products can ingest it through feeds or API integration.
Tactical intelligence is the easiest type of intelligence to generate and is almost always automated. As a result, it can be found via open source and free data feeds, but it usually has a very short lifespan because IOCs such as malicious IPs or domain names can become obsolete in days or even hours.
Data sources for TTI: It's important to note that simply subscribing to intel feeds can result in plenty of data, but offers little means to digest and strategically analyze the threats relevant to you. Also, false positives can occur when the source is not timely or of high fidelity.

Operational intelligence. (OTI) In the same way that poker players study each other's quirks so they can predict their

opponents' next move, **cybersecurity professionals study their adversaries**.
Behind every attack is a "who," "why," and "how." The "who" is called attribution. The "why" is called motivation or intent. The "how" is made up of the TTPs the threat actor employs. Together, these factors provide context, and context provides insight into how adversaries plan, conduct, and sustain campaigns and major operations. This insight is operational intelligence.
Machines alone cannot create operational threat intelligence. Human analysis is needed to convert data into a format that is readily usable by customers. While operational intelligence requires more resources than tactical intelligence, it has a longer useful life because adversaries can't change their TTPs as easily as they can change their tools, such as a specific type of malware or infrastructure.
Operational intelligence is most useful for those cybersecurity professionals who work in a SOC (security operations center) and are responsible for performing day-to-day operations. Cybersecurity disciplines such as vulnerability management, incident response and threat monitoring are the biggest consumers of operational intelligence as it helps make them more proficient and more effective at their assigned functions.
True operational threat intelligence gives defenders the chance to implement controls in advance and thwart assaults, making it the golden standard of security in so many aspects.
Even incomplete intelligence might offer important clues about impending attacks, for instance by pointing out potential **attack vectors** before they are deployed.

Data sources for OTI: As it's linked to specific threat strategies, there are exactly two ways to acquire OTI:
1. Nurturing human informants, probably through recruitment or penetration, within an active threat group; 2. Infiltrating and monitoring the communication of a threat group.
Among the most popular sources are:
•Internet chat rooms
•Social networks
•Private forums on the open web or dark web
More serious criminal operations are much more likely to take measures, whereas less advanced threat groups—particularly those motivated by ideology—are willing to communicate their strategies through fairly vulnerable methods.

Strategic Threat Intelligence (STI):
Adversaries don't operate in a vacuum — in fact, there are almost always higher-level factors that surround the execution of cyber attacks. For example, nation-state attacks are typically linked to geopolitical conditions, and geopolitical conditions are linked to risk. Furthermore, with the adoption of financially motivated Big Game Hunting, cyber-crime groups are constantly evolving their techniques and should not be ignored. In simple terms, strategic threat intelligence is a bird's-eye view of an organization's threat

landscape. Not concerned with specific actors, indicators, or attacks, it instead aims to help high-level strategists understand the broader impact of business decisions.

Strategic intelligence helps decision-makers understand the risks posed to their organizations by cyber threats. With this understanding, they can make cybersecurity investments that effectively protect their organizations and are aligned with its strategic priorities.
Data sources for STI: Strategic intelligence tends to be the hardest form to generate. Strategic intelligence requires human data collection and analysis that demands an intimate understanding of both cybersecurity and the nuances of the world's geopolitical situation. Strategic intelligence usually comes in the form of reports.

Open-source intelligence (OSINT)

- Threat intelligence feeds are a critical part of TI. Widely available online, these feeds record and track IP addresses and URLs that are associated with phishing scams, malware, bots, trojans, adware, spyware, ransomware and more. Open source threat intelligence feeds can be extremely valuable—if you use the right ones. While these collections are plentiful, there are some that are better than others.

Tools to generate and share intelligence among partner organizations, Countries, groups:

- **MISP**
- **TheHive**
- **Cortex**
- **Yeti**
- **Cuckoo Sandbox**
- **OpenCTI (Open Cyber Threat Intelligence)**
- **T-Pot**

Open-Source Threat Intelligence Feeds:

- **AlienVault Open Threat Exchange (OTX)**
- **Cyber Threat Intelligence Network (CTIN)**
- **Abuse.ch**
- **CIRCL (Computer Incident Response Center Luxembourg) Passive DNS and Passive SSL**
- **Spamhaus**
- **PhishTank**
- **Malware Domain List**
- **SANS Internet Storm Center (ISC)**

https://logz.io/blog/open-source-threat-intelligence-feeds/


Testing strategies
CalPolyPomona

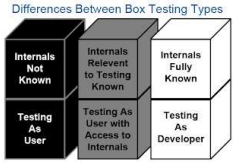
White hats: Penetration testing and testing modes

- ***Penetration testing*** (or ***pen testing***)**:** challenges a network's security. Given the value of a business's network, it is imperative that businesses consult with experts before pen testing. Experts can ensure that testing does not damage the network, and they can also provide better insights into vulnerabilities. Pen testing experts can help businesses before, during, and after the tests to help obtain useful and beneficial results.

•**White box testing** — in this format, pen testers have full access and knowledge of the systems they are testing, including source code, IP addresses, etc. Also sometimes called clear or open box testing, this approach can simulate an internal attack and allows for an extremely rigorous test.

•**Black box testing** — unlike white box scenarios, testers here have no information about the systems they will attempt to breach. Because of this, these tests often take longer to complete, as they may rely heavily on an automated, trial & error approach.

•**Gray box testing** — as the name indicates, this approach is a combination of the other two approaches. Testers have some visibility and can pose as an attacker who has gathered limited information about the target.

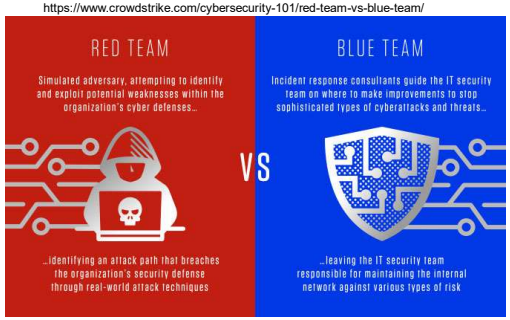


Red/Blue teaming

In a **red team/blue team** exercise, the **red team** is made up of offensive security experts who try to attack an organization's cybersecurity defenses. The **blue team** defends against and responds to the red team attack.

- Red team/blue team simulations play an important role in defending the organization against a wide range of cyberattacks from today's sophisticated adversaries. These exercises help organizations:
  - Identify points of vulnerability as it relates to people, technologies and systems
  - Determine areas of improvement in defensive **incident response** processes across every phase of the kill chain
  - Build the organization's first-hand experience about how to detect and contain a targeted attack
  - Develop response and remediation activities to return the environment to a normal operating state

https://www.crowdstrike.com/cybersecurity-101/red-team-vs-blue-team/



Examples of red team activities include:

- Performing **DNS research**
- Conducting **digital analysis** to create a baseline of network activity and more easily spot unusual or suspicious activity
- Reviewing, configuring and monitoring **security software** throughout the environment
- Ensuring **perimeter security methods**, such as firewalls, antivirus and anti-malware software, are properly

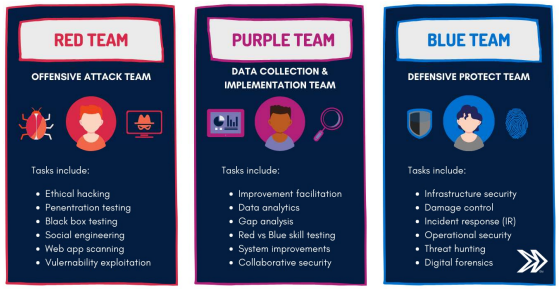
configured and up-to-date

- Employing **least-privilege access**, which means that the organization grants the lowest level of access possible to each user or device to help limit lateral movement across the network in the event of a breach
- Leveraging **microsegmentation**, a security technique that involves dividing perimeters into small zones to maintain separate access to every part of the network

Red vs Blue and Purple team

The Purple Team is, unsurprisingly, the joining of the insights from Red and Blue.

In the purple team, the offensive and defensive professionals work in sync. For instance, a purple team might decide to work on a particular security section; say, broken authentication. The offensive security professionals don't just start scouting for vulnerabilities. They work together with the defense to find out weak points and patch the vulnerabilities that might arise.



https://gomindsight.com/insights/blog/red-team-vs-blue-team/

https://www.makeuseof.com/what-is-purple-team-cybersecurity/

Observation: PenTester vs Red Team

- The main objective of penetration tests is to identify exploitable vulnerabilities and gain access to a system. On the other hand, in a red-team exercise, the goal is to access specific systems or data by emulating a real-world adversary and using tactics and techniques throughout the attack chain, including privilege escalation and exfiltration.

	Penetration testing	Red teaming
Objective	Identify exploitable vulnerabilities and gain access to a system.	Access specific systems or data by emulating a real-world adversary.
Timeframe	Short: One day to a few weeks.	Longer: Several weeks to more than a month.
Toolset	Commercially available pen-testing tools.	Wide variety of tools, tactics and techniques, including custom tools and previously unknown exploits.
Awareness	Defenders know a pen test is taking place.	Defenders are unaware a red team exercise is underway.
Vulnerabilities	Known vulnerabilities.	Known and unknown vulnerabilities.
Scope	Test targets are narrow and pre-defined, such as whether a firewall configuration is effective or not.	Test targets can cross multiple domains, such as exfiltrating sensitive data.
Testing	Security system is tested independently in a pen test.	Systems targeted simultaneously in a red team exercise.
Post-breach activity	Pen testers don't engage in post-breach activity.	Red teamers engage in post-breach activity.
Goal	Compromise an organization's environment.	Act like real attackers and exfiltrate data to launch further attacks.
Results	Identify exploitable vulnerabilities and provide technical recommendations.	Evaluate overall cybersecurity posture and provide recommendations for improvement.

https://www.ibm.com/blog/red-teaming-101-what-is-red-teaming/