Part 1 – Taxonomy of Cyber Attacks and Threats

Social Engineering Attacks

Social engineering attacks exploit human psychology and trust rather than technical vulnerabilities. Attackers impersonate trusted entities or offer enticing lures to trick victims into giving up information or access. They are common because even the strongest technical defenses can fail against human error.

- **Phishing:** A social engineering attack using fraudulent communication (e.g. emails or texts) that appears to come from a reputable source. The goal is to trick victims into divulging sensitive data (credentials, financial info) or installing malware. As of late, AI is being used to produce phishing emails and messages, facilitating the creation of phishing messages.
    - *Prevalence:* Extremely well-known and widespread.
    - *Targets/Vectors:* Targets individuals or employees via email (also via SMS "smishing" or voice calls "vishing"). Often cast a wide net; some campaigns target specific organizations (see spear phishing).
    - *Affected CIA Pillar:* Primarily **Confidentiality** (steals login credentials, personal data), but can lead to further compromise affecting **Integrity** (unauthorized transactions) or **Availability** (if malware like ransomware is installed).
    - *Exploited Vulnerability:* Human gullibility.
    - *Risk/Impact:* Very high. A successful phishing attack can lead to large-scale data breaches or financial losses.
    - *Prior Awareness:* All members of the group had prior awareness of this attack.
- **Spear Phishing & Whaling:** These are **targeted phishing** attacks. **Spear phishing** refers to highly customized phishing aimed at a specific person or small group, often after careful research of the target (fortinet.com). **Whaling** is a spear-phishing attack directed at “big fish” – high-value targets like C-suite executives (fortinet.com).
    - *Prevalence:* Well-known variants of phishing, increasingly common as attackers realize personalized lures yield higher success.

- *Targets/Vectors:* Targets **specific individuals** (e.g. an organization's CEO or finance manager) via personalized emails or messages that appear to come from trusted sources (colleague, partner, etc.). Whaling often impersonates executives or business partners to trick senior personnel.

- *Affected CIA Pillar:* **Confidentiality** is chiefly at risk. If credentials are stolen, subsequent misuse can affect **Integrity** of systems or **Availability** (e.g. fraudulent transfers, sabotage).

- *Exploited Vulnerability:* **Personalization blind spot**.

- *Risk/Impact:* High – a successful spear phishing can compromise privileged accounts or confidential data. Whaling can be devastating (e.g., facilitating large fraudulent wire transfers or releasing sensitive corporate information).

- *Prior Awareness:* None of the team members were previously aware of this attack.

Malware Attacks

"Malware" encompasses malicious software designed to infiltrate, damage, or exploit systems (cisa.gov). Malware attacks involve introducing such software into the target's system. Below are common malware types and their attack characteristics:

- **Computer Virus:** A type of **malicious code that attaches to files or programs** and spreads to other files or systems when those are shared or executed (fortinet.com). Viruses often execute unwanted functions like corrupting data or slowing systems.

  - *Prevalence:* Classic and well-known (viruses have existed since the 1980s). Less common today relative to worms or trojans, but still appear (especially macro viruses or infecting files on USB drives).

  - *Targets/Vectors:* Targets any users who execute infected files. Common vectors include email attachments, infected program downloads, or document macros. Human action (opening a file) is usually required to trigger a virus.

  - *Affected CIA Pillar:* Often **Integrity** and **Availability** – viruses can corrupt or delete data (integrity breach) and crash systems (affecting availability).

  - *Exploited Vulnerability:* **Inadequate malware scanning and user caution.**

  - *Risk/Impact:* Variable – some viruses are relatively benign pranks, but others (e.g., destructive ones like CIH or NotPetya) can have severe impact, destroying data or rendering systems unusable.

    - *Prior Awareness:* All members of the group had prior awareness of this attack.

- **Trojan Horse:** Malware **disguised as legitimate software** that the user is tricked into executing, thereby allowing the attacker to gain unauthorized access or control. When run, the trojan can open a backdoor or perform malicious actions while appearing harmless (fortinet.com).

    - *Prevalence:* Very common and well-known. Trojans are a **top threat** since many modern attacks use trojanized files (e.g., a game crack, or a document with hidden malware) to breach systems.

    - *Targets/Vectors:* Targets end users who download or run unvetted programs. Common vectors: email attachments claiming to be documents, software downloads from untrusted sites, pirated software, or even USB drives.

    - *Affected CIA Pillar:* **Confidentiality**, **Integrity**, and **Availability**. Many trojans create a backdoor for persistent access (ongoing confidentiality/integrity risk).

    - *Exploited Vulnerability:* **User trust and lack of verification.**

    - *Risk/Impact:* High – trojans often serve as a **first stage** in advanced attacks, enabling attackers to bypass security (since the user runs the malware willingly). They can lead to full system compromise. For example, a banking trojan can steal financial logins, or a Remote Access Trojan (RAT) can give attackers complete control over the machine.

    - *Prior Awareness:* All members of the group had prior awareness of this attack.

- **Ransomware:** A form of malware that **encrypts or locks victim's data** and demands a ransom payment for restoring access (or threatens to leak data if not paid) (cisa.govfortinet.com). Ransomware typically spreads like other malware (phishing emails, malicious downloads) but its defining feature is extortion via encryption.

    - *Prevalence:* Unfortunately **very well-known and on the rise** in recent years. It's one of the most prominent threats facing organizations and individuals alike, with numerous high-profile incidents.

    - *Targets/Vectors:* Targets all kinds of users – individuals, businesses, hospitals, even city governments. Often delivered via phishing attachments or links, exploit kits on compromised websites, or through trojans/worms that drop it.

    - *Affected CIA Pillar:* Primarily **Availability** (it denies access to data by encryption) and secondarily **Confidentiality** (some modern ransomware, aka

double-extortion, steals data to threaten publishing it).

- *Exploited Vulnerability:* **Weak user security and unpatched systems.**

- *Risk/Impact:* **Critical** – impact is immediate loss of access to critical data/systems. Entire businesses have been crippled for days or weeks. Financial impact is high (ransom payments, recovery costs) and there can be collateral damage like reputational harm or data leaks. For example, the **WannaCry** ransomware outbreak affected hundreds of thousands of systems worldwide, disrupting healthcare and other services (geeksforgeeks.org).

- *Prior Awareness:* All members of the group had prior awareness of this attack.

- **Spyware / Keyloggers:** Malware that **secretly monitors user activity and steals information**. This includes keyloggers that record keystrokes, as well as broader info-stealers that capture screenshots, credentials, or browser data (umbrella.cisco.com). These often operate stealthily to avoid detection while exfiltrating data.

  - *Prevalence:* Common component of many malware infections (well-known). Often spyware is part of trojans or installed by other malware. Commercial spyware also exists (stalkerware).

  - *Targets/Vectors:* Targets individuals' computers or phones to gather personal data (logins, credit cards, communications). Common vectors include trojans pretending to be useful software, malicious browser extensions, or attachments that install a keylogger.

  - *Affected CIA Pillar:* **Confidentiality** is directly impacted (it's all about stealing private information). It can also affect **Integrity** if attackers use stolen credentials to manipulate accounts, and **Availability** if the malware destabilizes the system, though stealth is usually a priority to keep spying.

  - *Exploited Vulnerability:* **Lack of anti-malware defenses and user unawareness.**

  - *Risk/Impact:* High for the individual or organization compromised – spyware can lead to **identity theft**, financial fraud, or espionage (if corporate). For example, keyloggers can capture passwords to banking sites or corporate VPNs, leading to further breaches.

  - *Prior Awareness:* some members of the group were previously aware of this attack.

Network & Infrastructure Attacks

Network-based attacks target the communication infrastructure, network protocols, or the availability of network services. They often aim to eavesdrop on, redirect, or disrupt data in transit. Below are key types:

- **Denial-of-Service (DoS) / Distributed DoS:** Attacks designed to **overwhelm a target system with traffic or requests**, exhausting its resources so that legitimate users cannot be served (fortinet.com). A **DDoS** uses many distributed sources (often a botnet of malware-infected machines) to amplify the traffic flood (fortinet.com).
    - *Prevalence:* Very well-known. DoS/DDoS attacks have been around for decades and remain common (especially DDoS, given the rise of botnets). They range from small nuisance attacks to massive internet-breaking events.
    - *Targets/Vectors:* Targets typically **servers, websites, or network infrastructure**. Common targets include web servers, DNS servers, or VoIP systems. Vectors include flooding the target with **voluminous traffic** (e.g., HTTP requests, UDP/TCP packets, ICMP pings) or exploiting protocol quirks (like DNS amplification).
    - *Affected CIA Pillar:* **Availability** exclusively – the goal is to make the service unavailable to legitimate users.
    - *Exploited Vulnerability:* **Capacity limits and protocol weaknesses.**
    - *Risk/Impact:* Ranges from moderate to severe. For an e-commerce site or online service, a sustained DDoS can mean huge business losses (downtime). Critical infrastructure (banks, government sites) going down can have public safety or economic impacts.
    - *Prior Awareness:* All members of the group had prior awareness of this attack.
- **Man-in-the-Middle (MITM):** An attack where the adversary **secretly intercepts or alters communications** between two parties, positioning themselves in the "middle" (fortinet.com). The victims believe they are directly communicating with each other, unaware of the eavesdropper/forger in between.
    - *Prevalence:* Well-known category of attacks, with various forms (Wi-Fi eavesdropping, HTTPS spoofing if certificates are not validated, etc.). While improved encryption (TLS) has reduced some MITM, it's still a real threat especially on unsecured networks.
    - *Targets/Vectors:* Targets any two-party communication (client-server or peer-to-peer). Common scenarios: intercepting data on public Wi-Fi, ARP spoofing on a LAN to spy on local traffic, or DNS spoofing to misdirect users (a related attack described separately below). Vectors include network impersonation (rogue Wi-Fi access point), address spoofing (ARP/DNS

tricks), or session hijacking techniques.

- *Affected CIA Pillar:* **Confidentiality** and **Integrity**. Availability is usually not the goal, though MITM could lead to downtime if communications are blocked or tampered with.

- *Exploited Vulnerability:* **Lack of authentication and encryption in communications.**

- *Risk/Impact:* High if successful – the attacker can steal sensitive data (passwords, financial info) or inject malicious instructions (e.g., altering a bank transaction detail mid-transfer). An infamous example is attackers intercepting online banking sessions to perform fraudulent transactions.

- *Prior Awareness:* All members of the group had prior awareness of this attack.

Web & Application Attacks

These attacks exploit vulnerabilities in software applications, especially web applications, to gain unauthorized access, manipulate data, or execute malicious code. They often leverage improper input handling or flaws in application logic.

- **SQL Injection:** An attack where the attacker **inserts malicious SQL code** into a query by manipulating user input (such as a form field), causing the backend database to execute unintended commands (fortinet.com). This can result in unauthorized data access or damage to the database.

  - *Prevalence:* Very well-known and one of the **top web application vulnerabilities** for decades. Despite awareness, SQL injection still appears frequently in poorly secured apps. It's been responsible for many major data breaches.

  - *Targets/Vectors:* Targets web applications (or any app using an SQL database) that directly include user inputs in SQL queries without proper sanitization. Common vectors: web forms (login forms, search boxes, URL parameters) where an attacker inputs specially crafted SQL syntax (like `' OR '1'='1` to bypass authentication or `'; DROP TABLE users;--` to delete data).

  - *Affected CIA Pillar:* **Confidentiality** (can extract sensitive data like user credentials), **Integrity** (attackers can modify or delete database records), sometimes **Availability** (SQLi can be used to destroy data or even crash a database, knocking a service offline).

  - *Exploited Vulnerability:* **Lack of input validation and parameterization.**

    - *Risk/Impact:* **Critical.** A successful SQL injection can dump entire databases (e.g., all usernames/passwords from a site) or erase them. Many notorious breaches (e.g., of retailers, financial orgs) have occurred via SQLi, leaking millions of records.

    - *Prior Awareness:* All members of the group had prior awareness of this attack.

- **Cross-Site Scripting (XSS):** An attack where malicious scripts are **injected into benign websites** such that they execute in other users' browsers (fortinet.com). Typically, an attacker exploits a web application that doesn't sanitize user-generated content (like comments or profile fields) to deliver a script to other users, which runs in their context (often stealing cookies or altering page content).

    - *Prevalence:* Very common and well-known (another OWASP Top 10 staple). There are different types (Stored XSS, Reflected XSS), but all revolve around executing scripts in the victim's browser. Despite being around for a long time, XSS remains widespread in poorly sanitized web apps.

    - *Targets/Vectors:* Targets **users of a web application** by using the application as the delivery mechanism. Vectors include injecting JavaScript into web pages – e.g., posting a malicious `<script>` in a forum, or sending a specially crafted URL that a user clicks (for reflected XSS).

    - *Affected CIA Pillar:* Primarily **Confidentiality** (often used to steal session cookies or credentials from the user's browser) and **Integrity** (can manipulate what the user sees or even perform actions on their behalf, like changing account settings). **Availability** isn't typically targeted, though theoretically an XSS could inject a logic to redirect or freeze the page for the user (a minor availability issue).

    - *Exploited Vulnerability:* **Improper output encoding and input validation by web applications.**

    - *Risk/Impact:* Medium to high – depends on the context. In worst cases, XSS can **hijack user accounts** (steal cookies/session tokens leading to impersonation) or spread like a worm (if the script self-propagates, as occurred on some social networks in the past). It can also be used for **phishing** (displaying fake login forms on a legit site) or simply defacing a site for those users.

    - *Prior Awareness:* Some members of the group were previously aware of this attack.

- **Cross-Site Request Forgery (CSRF):** An attack that tricks a user's browser into **unwittingly executing actions** on a web application where they're authenticated, by leveraging the user's session. The attacker crafts a malicious request (for example,

an HTTP form submission) and pushes the victim's browser to send it (via image tags, hidden forms, etc.), causing the web app to perform an action as the user (since the browser includes the user's session cookies automatically) (fortinet.com).

- *Prevalence:* Well-known in web security circles, though less publicized than XSS/SQLi. Many modern frameworks include CSRF defenses by default now (tokens), but it still surfaces in custom or older apps.

- *Targets/Vectors:* Targets **state-changing actions** on websites (e.g., initiating a funds transfer, changing an email address, posting a message) where the user is already logged in. Vectors include malicious links or code that the user either clicks or that auto-loads (like an HTML image that triggers a GET request). For instance, an attacker might email a victim a seemingly innocuous image link that actually triggers a money transfer on a bank site if the victim is logged in to online banking.

- *Affected CIA Pillar:* **Integrity** is the primary pillar affected (unauthorized commands are executed, altering data or state).

- *Exploited Vulnerability:* **Absence of proper request authentication (CSRF tokens or checks).**

- *Risk/Impact:* Medium to high – depending on the action that can be forged. If a critical transaction (like financial transfer or account change) lacks CSRF protection, the impact can be severe (money theft, account takeover by changing email/password). However, CSRF typically requires the victim to be in a logged-in session and to click a link or visit a malicious page, which adds some constraints.

- *Prior Awareness:* None of the group members were previously aware of this attack.

- **Buffer Overflow:** An attack against native software (often written in C/C++) where an attacker provides **input that overruns a buffer's boundary in memory**, overwriting adjacent memory and potentially injecting executable code (imperva.com). This often leads to **arbitrary code execution**, allowing the attacker to take control of the program or system.

  - *Prevalence:* A classic low-level attack – well-known historically as one of the main software exploitation techniques. Still relevant (especially in systems software, embedded, or any unsafe memory-handling context), though memory-safe languages and modern OS protections have reduced incidence. Many older worms and exploits (like Code Red, Slammer) used buffer overflow vulnerabilities.

  - *Targets/Vectors:* Targets any program that handles external input in insecure languages. Common targets: network services (daemons) written in C that parse data (e.g., old FTP, HTTP servers), client applications processing files

(media players, image libraries), and even local privilege escalation exploits in OS components.

- *Affected CIA Pillar:* **Integrity** (the attacker injects their own code/commands by corrupting memory) and **Confidentiality** (if they take control, they can access data).

- *Exploited Vulnerability:* **Memory safety weaknesses in software.**

- *Risk/Impact:* High – a buffer overflow in a widely used service can lead to major compromises. For instance, the **WannaCry** ransomware spread using the EternalBlue exploit, which was essentially a buffer overflow in Windows SMB service, allowing complete system takeover. Successful exploitation can give an attacker the same privileges as the affected program (which, if it's a privileged service, means a full system compromise).

- *Prior Awareness:* All members of the group had prior awareness of this attack.

Identity and Credential Attacks

These attacks focus on breaking authentication mechanisms or misusing stolen credentials to gain unauthorized access. They often do not involve exploiting a software flaw, but rather weaknesses in human password choices or credential management.

- **Brute-Force Attack (Password Cracking):** A trial-and-error method where attackers **systematically attempt many possible passwords or keys** until the correct one is found (fortinet.com). Simple brute-force tries every combination, while more efficient variants use dictionaries of common passwords or clever guesses (personal info, etc.).

  - *Prevalence:* Well-known and very common, especially against online accounts with weak passwords. Automated tools make brute-forcing easy, though many systems now have lockout policies to limit it. Brute force is also used offline (e.g., cracking hashed password files or Wi-Fi keys) where no lockout can intervene.

  - *Targets/Vectors:* Targets **authentication systems**. Online brute force might target a login page or an SSH service by repeatedly trying credentials. Offline, an attacker might obtain a list of hashed passwords (say from a leaked database) and then attempt to crack those hashes by guessing passwords. Vectors include using bots to distribute guesses or leveraging leaked password databases to speed up guessing (the attacker may prioritize

guesses like “Password123” or known leaked passwords).

    - *Affected CIA Pillar:* **Confidentiality** – if the password is obtained, the attacker can breach account confidentiality (and possibly integrity by performing actions in the account).

    - *Exploited Vulnerability:* **Weak passwords and lack of account lockout.**

    - *Risk/Impact:* Moderate to high. If accounts have **weak passwords**, brute force can result in account compromise – for a user, that could mean email or social media hacked; for an admin account, a complete system takeover. The impact depends on the privileges of the account. In the worst case, a successful brute force on an administrator password can compromise an entire domain or critical system.

    - *Prior Awareness:* All members of the group had prior awareness of this attack.

- **Credential Stuffing:** A specialized attack where attackers **take lists of known compromised username/password pairs** (from past data breaches) and try them on other services, banking on password reuse (imperva.com). Unlike brute force (which guesses new passwords), credential stuffing uses real credentials that have leaked, just in new places.

    - *Prevalence:* Emerged prominently in the last decade due to the plethora of data breaches leaking billions of credentials. Now very common and a major threat to any online service (given many users reuse passwords). It’s a leading cause of account takeover incidents.

    - *Targets/Vectors:* Targets **online services** with login functionality – from email and banking to streaming services. The vector is an **automated login attempt** – attackers use bots to inject stolen credentials at scale into login forms of target websites, looking for hits. For example, using a dump of LinkedIn passwords to try to log in to Gmail, knowing many people reuse the same email/password.

    - *Affected CIA Pillar:* **Confidentiality** (unauthorized access to user accounts means viewing private information) and **Integrity** (the attacker can perform actions or changes within those accounts – e.g., transfer funds, send emails, etc.).

    - *Exploited Vulnerability:* **Human password reuse and lack of multi-factor authentication.**

    - *Risk/Impact:* High – credential stuffing is a very efficient way for attackers to break into accounts. Given large breach datasets, even a small success rate (say 0.1%) can yield thousands of compromised accounts. For organizations, if employees reuse corporate passwords elsewhere, credential stuffing can

lead to breaches of the corporate network (this is why password reuse is dangerous).

- *Prior Awareness:* All members of the group had prior awareness of this attack.

Other Notable Threats and Attack Vectors

Finally, some attacks don't fit neatly into the above technical categories or are higher-level threat concepts. These often involve multiple techniques or target the broader ecosystem around a target.

- **Supply Chain Attacks:** Instead of attacking a target directly, adversaries **compromise a trusted third-party** (software vendor, IT service provider, hardware supplier) that the target relies on (crowdstrike.com). By tampering with products or updates, attackers infiltrate many victims through one breach of the supply chain. For example, inserting malware into a software update that is pushed out to thousands of customers.
  - *Prevalence:* This is an **increasingly emergent threat** in recent years. Famous incidents like the SolarWinds Orion compromise (2020) brought supply chain attacks to the forefront. Previously considered rare and advanced, they are now a major concern for organizations globally.
  - *Targets/Vectors:* Targets **software supply chains** (e.g., compromising an app's code or updates), **hardware supply chains** (infecting devices or components before delivery), or other suppliers (like a payroll service provider to get into many client companies). Vectors vary: inserting malicious code into open-source libraries that many projects use, hacking into a vendor's build system to trojan an update (as happened with SolarWinds), or even planting backdoors in hardware/firmware during manufacturing.
  - *Affected CIA Pillar:* Potentially **all pillars** depending on the attack. Often **Confidentiality** and **Integrity** are prime. **Availability** can be affected if the compromised product is used to disrupt services.
  - *Exploited Vulnerability:* **Trust relationships** and **complex software dependencies**.
  - *Risk/Impact:* **Very high.** These attacks can have a sweeping impact because one successful supply chain compromise can infect thousands of organizations. For instance, the SolarWinds attack inserted a backdoor that affected numerous government agencies and companies worldwide. Impact includes large-scale espionage (stealing data from many victims) and potentially sabotage.

    - *Prior Awareness:* No members of the group were previously aware of this attack.

- **Insider Threats:** Unlike external attacks, this refers to threats originating from **within the organization** – e.g., a rogue employee or contractor misusing their access (fortinet.com). Insiders might steal data, facilitate malware entry, or sabotage systems, either out of malice (espionage, revenge, profit) or accidentally through negligence.

    - *Prevalence:* Unfortunately common and well-recognized in security. Many breaches are caused or aided by insiders, sometimes unwittingly (phished employees, or mistakes) and other times intentionally (disgruntled or bribed staff). Every organization faces insider risk to some degree.

    - *Targets/Vectors:* The target is the organization's **internal assets**, but since the actor is an insider, the "vector" is their legitimate access. For malicious insiders, they might copy confidential files to external drives (data exfiltration), provide their login to attackers, or even directly modify/delete data.

    - *Affected CIA Pillar:* Potentially **all three**. An insider can steal data (breaching confidentiality), alter or destroy information (integrity), or disrupt operations (availability).

    - *Exploited Vulnerability:* **Trust and privilege**.

    - *Risk/Impact:* Very high. Insiders can be one of the most damaging threat sources because they may already have the "keys to the kingdom." An angry system administrator, for instance, could cause massive outages or data loss. A coerced or bribed employee might leak thousands of customer records.

    - *Prior Awareness:* All members of the group had prior awareness of this attack.

- **Advanced Persistent Threat (APT):** APT refers less to a specific attack and more to **an advanced, stealthy adversary (often nation-state or organized group) that targets a specific entity and sustains a long-term intrusion (**umbrella.cisco.com). APTs typically blend multiple techniques (phishing, zero-day exploits, custom malware) and carefully cover their tracks to maintain persistent access inside the target network for espionage or sabotage.

    - *Prevalence:* Well-known in the cybersecurity field as the label for the most sophisticated breaches. APT incidents (like those attributed to state-sponsored hacking groups) have been on the rise. For the general public, APT became a buzzword after attacks like Stuxnet or the RSA breach; now in 2025, it's common to hear about nation-state hackers or "advanced threats" in the news.

- *Targets/Vectors:* Targets are usually **high-value organizations**: governments, defense contractors, critical infrastructure, or corporations with valuable IP. Vectors are numerous and **often custom-tailored** – spear phishing emails carrying zero-day malware, watering-hole attacks, supply chain compromises, and even physical methods if needed (like an infected USB drop). APT groups often exploit **previously unknown vulnerabilities (zero-days)** to infiltrate, since they have resources to discover or purchase such exploits.

- *Affected CIA Pillar:* **Confidentiality** is a primary focus (stealing sensitive information/intellectual property or state secrets). **Integrity** can also be targeted (e.g., an APT might quietly alter data or sabotage systems, as in attacks on industrial control systems).

- *Exploited Vulnerability:* **Multi-faceted** – any weakness that can be found. This includes technical vulnerabilities, **social vulnerabilities** and weaknesses in monitoring. A hallmark is exploiting **zero-day vulnerabilities** giving no opportunity for the target to have patched. They also exploit trust to move laterally inside networks.

- *Risk/Impact:* **Critical and far-reaching.** If you're targeted by an APT, the impact can be enormous. APTs may persist for months or years quietly, so the long-term breach can mean a complete loss of privacy and security for the target environment.

- *Prior Awareness:* Not applicable, since it is not a concrete kind of attack.

Part 2 – Cybercrime Landscape

Cybercrime Entities

- **Insiders:** Employees, contractors, or partners abusing their legitimate access to a company's assets.
  - *Motivations:* Revenge, ideology, personal gain (selling data), coercion (blackmail/bribes).
  - *Targets:* the company and its affiliates.
  - *Modus operandi:* Leak sensitive data, sabotage systems, misconfigure security settings, sell credentials to criminals.
  - *Example:* Edward Snowden, who leaked NSA classified data.
- **Individuals:** Amateur or self-taught attackers acting alone, often driven by curiosity, ego, or the thrill of breaking systems. They typically lack advanced skills and rely on prebuilt tools.
  - *Motivations***:** Curiosity, reputation, challenge, small profits.
  - *Targets***:** Personal accounts, small websites, gaming platforms, peers.

    - *Modus operandi***:** Use off-the-shelf tools (phishing kits, password crackers), exploit simple misconfigurations, deface sites, steal credentials to resell or boast.
    - *Example:* Gary McKinnon, a UK hacker who breached US military systems alone.
- **Small groups:** 2–10 people collaborating informally, often running short-term fraud or phishing operations with role specialization.
    - *Motivations:* Financial profit, side income, notoriety.
    - *Targets:* small companies, freelancers, consumers, social media accounts.
    - *Modus operandi:* Spear-phishing, business email compromise (BEC), romance scams, fake e-commerce sites, investment fraud; use leaked credentials and basic malware bought online.
    - *Example:* Scattered Spider, a teen/young adult social-engineering crew behind several 2023 data breaches.
- **Organized groups/mafias:** Structured, profit-driven cybercriminal organizations operating like full-fledged businesses. Some evolved entirely online, while others are cyber branches of traditional organized crime groups. They run persistent, large-scale operations with clear hierarchies, specialisation, and global infrastructure.
    - *Motivations:* Systematic long-term profit, financial dominance, sometimes intimidation or territorial control.
    - *Targets:* Large companies, financial entities, high-net worth individuals.
    - *Modus operandi:* Large-scale phishing, credential theft, ransomware/extortion, laundering through shell companies and crypto.
    - *Examples:* LockBit (a RaaS cartel with global affiliates and corporate-style structure), Carbanak (Eastern European gang that stole hundreds of millions from banks via ATM and POS malware).
- **State-sponsored Groups:** Highly resourced teams affiliated with national intelligence or military agencies, often called “Advanced Persistent Threats” (APTs). They conduct long-term operations to achieve strategic, political, or military objectives, rather than immediate financial gain.
    - *Motivations:* Espionage, strategic disruption of adversaries, influence operations, military advantage, and economic competition.
    - *Targets:* Government institutions, critical infrastructure, defense contractors, telecom and tech companies, political organizations, media, and research institutes.
    - *Modus operandi:* Custom malware, zero-day exploits, supply-chain compromises, long-term stealthy intrusions.
    - *Examples:* Lazarus Groups (a North Korean group involved in espionage, bank heists, crypto theft, etc.), APT (a Russian group focussed on intelligence collection).

Counter Crime Entities

- **Individual defenders:** Independent researchers and ethical hackers, mostly hobbyists.

    - *Specificity*: Cyber-specific.
    - *Threat coverage*: Broad, generally low-complexity.
    - *Examples*: Independent bug bounty hunters on platforms like *HackerOne* or *Bugcrowd*; volunteer networks like *The Shadowserver Foundation*.
- **Corporate security teams:** Security teams and private companies that protect their own infrastructure or sell defensive services.
    - *Specificity*: Cyber-specific.
    - *Threat coverage*: Broad but business-focussed. They protect the companies' technological assets against intrusion, data theft, DDoS, etc.
    - *Examples*: Security Operations Centers (SOCs) at large companies (e.g. Google).
- **National cybersecurity agencies and CERTs:** Government defense organizations responsible for national-level defense and incident response.
    - *Specificity:* Cyber-specific.
    - *Threat coverage:* Broad.
    - *Examples:* **ENISA** (EU-wide analysis and capacity building), **CCN-CERT** in Spain, **CISA** in the US.
- **National law enforcement agencies:** Police and investigative bodies with dedicated cybercrime units.
    - *Specificity:* General law enforcement (often with specialized cybersecurity branches).
    - *Threat coverage:* Broad.
    - *Examples:* **FBI Cyber Division** in the US, **Brigada de Investigación Tecnológica (BIT)** in Spain.
- **International coordination bodies:** Supranational organizations linking national forces and sharing intelligence.
    - *Specificity:* General law enforcement with cyber-focused programs.
    - *Threat coverage:* Broad.
    - *Examples:* **INTERPOL Cybercrime Directorate** (global), **Europol EC3** (European Union).

Sources: The information above was gathered and synthesized from a variety of cybersecurity resources and references, including definitions and examples from Cisco, CISA, CrowdStrike, Fortinet, Imperva, and others. Key points are supported by the following sources:

- Cisco (Cybersecurity Threats and Advisories) – definitions of malware, phishing, ransomware (cisa.govcisco.com).
- CrowdStrike – explanation of social engineering and specific techniques like baiting, pretexting, tailgating (crowdstrike.comcrowdstrike.comcrowdstrike.com).
- Fortinet (Cyber Glossary and blog) – descriptions of various attack types (DDoS, phishing variants, ransomware, etc.) (fortinet.comfortinet.comfortinet.com).
- Imperva – details on web attacks such as SQL injection, XSS, CSRF, buffer overflow (fortinet.comfortinet.comimperva.com).
- CISA – overview of common attacks (malware, phishing) (cisa.gov).
- CrowdStrike (Supply Chain Attack article) – supply chain definition and context (crowdstrike.com).
- Fortinet (Insider Threat article) – insider threat definition and impact (fortinet.com).
- Cisco Umbrella – definitions of info-stealers, APTs (umbrella.cisco.comumbrella.cisco.com).
- Imperva (Learning Center) – credential stuffing definition (imperva.com).

Each specific attack entry in the taxonomy references these or other relevant sources to ensure accuracy and clarity. The citations (in square brackets) point to the lines in the source material that substantiate the information provided.

biblia: https://arxiv.org/pdf/2401.01374

https://www.fairinstitute.org/hubfs/FAIR%20CRM%20Body%20of%20Knowledge/FAIR%20Institute%20--%20Cyber%20Risk%20Scenario%20Taxonomy%20(February%202025).pdf