**ATTACK TAXONOMIES**

There are different types of attack taxonomies that can be categorized into the following.

**Network-based attacks**: They aim at the network infrastructure, trying to steal data or gain access to it, for example. Examples: Denial-of-Service (DoS), Man-in-the-middle (MITM) or Packet sniffing.

**Malware-based attacks**: The main idea is to use malicious software to infect devices.

**Web-based attacks**: They target websites and browsers. Examples: Cross-site scripting (XSS) or SQL injection.

**Attacks targeting operating systems**: As the name suggests, they attack the vulnerabilities in the different OS, typically to execute malicious code or steal data. Examples: Kernel-level attacks, Buffer overflow attacks or Privilege escalation attacks.

**Wireless and mobile attacks**: They exploit vulnerabilities in the network and the physical mobile devices. Examples: Wi-Fi attacks, Bluetooth attacks or SMS phishing (smishing).

**Social engineering**: They are based on human factors. The main idea is to manipulate people in order to make them pay or give the data. Examples: Phishing, Baiting or Scareware and fake alerts.

**Insider attacks**: As social engineering, it is based on people attacks. They are usually employees or partners that have access to private data. Examples: Unauthorized access or sabotage.

In this document we will look more specifically at Malware, because we think that it is the most known one.

| ***Rootkits and backdoors*** | |
| --- | --- |
| Brief description | **Rootkit**: Collection of malicious code that **hides in privileged areas** of the system and masks its execution to avoid detection. There are different types of rootkits depending on the level of privilege they execute on.  **Backdoor**: Hidden method to bypass authentication in a system and allow remote access.  A rootkit hidden in an infected computer can install a backdoor to allow the attacker full access to the system. |
| Are well-known attacks or emergent ones? | Both are well-known. |
| Identify targets, sources, vectors | Typical targets may be personal computers, IoT devices, enterprise servers, etc.  These kinds of malware can come from different sources, it can be distributed by cybercrime organizations, state-sponsored groups, etc.  The attack vector also varies. To install a rootkit or obtain a backdoor, the attacker must first gain access to the system, which can be done by exploiting a vulnerability, a misconfiguration, using social engineering, a trojan, etc. |
| Which pillar/s they aim at affecting: confidentiality, availability, integrity? | They mostly affect confidentiality. |
| Which vulnerability they aim at exploiting? | They do not target a particular vulnerability, but they allow an attacker remote access to the infected system. |
| Additional characteristics such as risk, impact | Rootkits are not too common nowadays due to the multiple kernel protections that are available today, so there’s little risk of infection. Backdoors however are widely used and integrated in other types of malware.  Backdoors and rootkits can have a critical impact in the infected system. They can be used to exfiltrate data, infect the system with more malware, spread malicious software and more. |
| Did you know this attack before doing this activity? | Yes. |
| Examples | **Ramen Rootkit**: A specific type of linux rootkit that mostly targeted RedHat systems. It operated at the kernel level, and would replace legitimate system binaries with malicious versions. Its main goal was to maintain unauthorized access and control to the system, and served as a platform to launch additional attacks and download/execute payloads.  An example of an attack where a backdoor was used is the **SolarWinds Orion Platform attack**. |

|  | ***Ransomware*** |
| --- | --- |
| Brief description | What Ransomware does is encrypt files of an organization / personal files, demanding some payment to unencrypt them. |
| Are well-known attacks or emergent ones? | They are well-known. There have been recent attacks on large entities in Barcelona, such as UAB or Hospital Clínic. In the Hospital Clínic, apart from asking for money, they also published private data. |
| Identify targets, sources, vectors | The usual target is big organizations. |
| Which pillar/s they aim at affecting: confidentiality, availability, integrity? | They are aiming for the 3 pillars at the same time. |
| Which vulnerability they aim at exploiting? | Weakness on systems, software or human behavior to encrypt data. |
| Additional characteristics such as risk, impact | They have high risk, because of all the potential data loss. |
| Did you know this attack before doing this activity? | I remember some attacks like the UAB one, but I didn’t know it was specifically a Ransomware attack. |
| Examples | Apart from the ones I mentioned before, WannaCry was a ransomware that attacked numerous hospitals, stealing their data and asking for money. This ransomware was made possible by a Microsoft vulnerability, EternalBlue, that allowed attacks to some not updated Windows computers and servers. |

<https://nordvpn.com/cybersecurity/glossary/attack-taxonomy/>

<https://www.bancosantander.es/glosario/ransomware>

<https://www.clinicbarcelona.org/ca/premsa/ultima-hora/ciberatac-a-lhospital-clinic-barcelona>

**Botnets and command-and-control (C&C) attacks**

a. Brief description

b. Are well-known attacks or emergent ones?

c. Identify targets, sources, vectors

d. Which pillar/s they aim at affecting: confidentiality, availability, integrity?

e. Which vulnerability they aim at exploiting?

f. Additional characteristics such as risk, impact

g. Did you know this attack before doing this activity?

| ***Botnets and command-and-control (C&C) attacks*** | |
| --- | --- |
| Brief description | C&C: Consist in creating a covert link between the compromised system and a C&C server. This connection allows prolonged access to control and execute malicious activities remotely.  Botnets: A botnet is a network of infected computers or IoT devices that an attacker can control remotely. Used to launch large-scale attacks using all the resources of the botnet. |
| Are well-known attacks or emergent ones? | Well-known attacks. |
| Identify targets, sources, vectors | Any device connected to the internet is a potential target, including computers, IoT devices, and servers.  The sources can vary, ranging from cybercriminal organizations and governments to insiders within an organization.  Devices can be infected through various methods, such as malware delivered via phishing emails, drive-by downloads, or by exploiting vulnerabilities in software. |
| Which pillar/s they aim at affecting: confidentiality, availability, integrity? | They can affect all three pillars, but primarily availability (through DDoS attacks), confidentiality (data theft), and integrity (modifying or corrupting data). |
| Which vulnerability they aim at exploiting? | Vulnerabilities in software (unpatched systems), weak or default credentials, unprotected IoT devices, or phishing/social engineering tactics. |
| Additional characteristics such as risk, impact | The risk is high due to the wide-ranging damage that large botnets can cause. Impacts include service outages (DDoS), data breaches, and financial loss for companies. Botnets are difficult to dismantle due to their decentralized nature. |
| Did you know this attack before doing this activity? | Yes. |
| Example | One famous example is the **Mirai Botnet** attack in 2016. Mirai infected IoT devices, such as security cameras and home routers, by exploiting default credentials. The botnet was used to launch massive Distributed Denial of Service (DDoS) attacks, most notably against the DNS provider Dyn, causing major internet services like Twitter, Netflix, and Reddit to go offline for hours.  This attack demonstrated the vulnerability of IoT devices and the scale of damage that botnets can cause. |

<https://www.paloaltonetworks.com/cyberpedia/command-and-control-explained>

<https://www.tripwire.com/state-of-security/what-are-command-and-control-attacks>

<https://www.fastly.com/es/learning/what-is-a-botnet>

<https://www.humansecurity.com/learn/blog/9-of-the-most-notable-botnets>

<https://www.wallarm.com/what/what-is-a-botnet>

<https://www.comparitech.com/blog/information-security/command-and-control-attacks/>

<https://threatintelligencelab.com/cyber-attack-cycle/command-and-control-c2/>

<https://www.a10networks.com/blog/5-most-famous-ddos-attacks/>

| ***Virus, worms, Trojans*** | |
| --- | --- |
| Brief description | **Virus**  Code fragment that copies its content in a program of the host. The code attacks other programs afterwards.  **Worm**  Independent program that reproduces by copying itself from one device to another, usually through the Network.  **Trojan**  Program that gives the attacker remote access to the infected host. |
| Are well-known attacks or emergent ones? | Well-known. |
| Which pillar/s they aim at affecting: confidentiality, availability, integrity? | All of them. |
| Identify targets, sources, vectors | Targets: Personal computers: From general users to big companies.  Sources: From particulars that sell the code to big cybercrime organisations.  Vectors: Executables, Email attachements, shared media, infected software, malicious websites, Social engineering |
| Which vulnerability they aim at exploiting? | System vulnerabilities, email attachments, file execution, Network vulnerabilities |
| Additional characteristics such as risk, impact | Data corruption or loss, decrease system performance, unauthorized access, system compromise, spread of more Malware, System control, Reputation damage… |
| Did you know this attack before doing this activity? | Yes, but I wasn’t sure about the differences between the three of them. |
| Examples | **Virus**  ILoveYou: It worked by sending a “Love letter” and sent itself to all contacts of the infected machine. The virus stole passwords of the victims.  **Worm**  MyDoom: Spread by mass Emailing. Mydoom sent copies of itself to addresses known by the infected machine. It caused several DoS attacks.  **Trojan**  Zeus trojan: It infected other machines via Phishing. It acts as a vehicle for all sorts of malicious payloads instead of doing the damage by itself. |

<https://www.javatpoint.com/virus-vs-worm-vs-trojan-horse>

<https://www.hp.com/us-en/shop/tech-takes/top-ten-worst-computer-viruses-in-history>

<https://www.digicert.com/faq/vulnerability-management/what-is-the-difference-between-viruses-worms-and-trojan-horses>

<https://www.bbc.co.uk/bitesize/guides/zs2y39q/revision/2>

**Sources:**

<https://attack.mitre.org/>  
<https://nordvpn.com/cybersecurity/glossary/attack-taxonomy/>

<https://www.clinicbarcelona.org/ca/premsa/ultima-hora/ciberatac-a-lhospital-clinic-barcelona>

[Rootkits & Backdoors]

<https://en.wikipedia.org/wiki/Rootkit>

<https://www.sans.org/blog/linux-incident-response-introduction-to-rootkits/>

<https://www.twingate.com/blog/glossary/backdoor%20attacks>

<https://www.ibm.com/es-es/topics/ransomware>