Introduction:

I chose to make the subject about payloads, how their made, and how they are hidden, and also how hackers are able to trick their victims into letting them into their system, and what they are able to do after with the victim's device.

What are payloads?

A payload is harmful code (malware) the hacker intends to send to the targeted device, it is the part of the malicious program that executes the unwanted action in the device.

How to make a payload?

Their are many ways and tools used to make payloads, but in my experience, the msfvenum tool in metasploit is quite useful, it's also one of the more popular tools to make a payload, if you were to use this tool, you would have to specify the operating system this payload is used for.

For example, when i tried to make a payload, i designed it for android, and a .apk file was created, you would later need to use keytool to generate a key and answer a few questions, and then you will need jarsigner to manually sign the .apk file, these last 2 steps are essesntial so the android system will trust the file (systems are getting better against cyberattacks so in this might not work in the near future).

In an other experience i had, i use the byonb (build your own botnet) tool to create a .py payload and another .exe payload to add a victim's computers to my botnet (my own computer).

How to hide a payload?

In the case of the msfvenom payload, you first have to hide the file within another application so i hid it in a android game file, to do this i could've used a many tools but i decided to use the embed tool which you can find in github, using the terminal i injected the the malicious file in the game file.

How to upload the payload to the device?

This tends to be the hardest part of the whole process but there are many ways to do this: *Social engineering: this includes tricking the victim into download the malicious file either by grabbing the victim's attention by making them click a shady link or the file itself, or you could send the a file to the victim directly in a scam type of fashion. *Vulnerabilities: a vulnerability is a hacker's best friend, they can be exploited as a result of a mistake in the code which will allow for attacks such a sql injection and xss. I didn't do any of this since i was just trying this out on my phone and computer.

What can a hacker do?

Using byob (the tool mentioned earlier) i was able to do a bunch of things with my computer (list in the post exploitation modules section) like: *Use it as part of a botnet that can be later used in a DDOS attack. *Bitcoin miner. *Keylogger. *Being able to see outlook emails. *Acces the webcam.

Conclusion:

Payloads are is an essential part of a malicious program and is probably the most dangerous thing in the cybersecurity domain since it can inflict a lot of damage like ransomware did a while back so you should be cautious of downnlaoding any suspicious files.