Subject :

PAGE NO.:
DATE:

# Know your enemy

→ everyone is equally likely to get attacked. Hackers run automated softwares to look for vulnerability across globe
→ A hacked email can be used for various dangerous activities
→ There are vulnerabilities in codes that can be exploited by hackers to seek information.
→ There can be special lines of code on website that can exploit your PC as soon as you open that site.
→ Known vulnerabilities have patches. If you have that patch, that vulnerability cannot be exploited.
→ Unknown bugs have no patch.
→ Vulnerabilities are assigned CVE numbers and their exploit code is available on the internet. Most of them are known vulnerabilities & therefore have patches.
→ If a person doesn't has the patch, they are likely to get attacked using the exploit code.

## ★ Current Threat Landscape:

↳ Hackers, Crackers & Cyber Criminals are [for] the top of the threat landscape.
- White Hat hackers are the people who are ethically paid by a company to target their servie for vulnerabilities.
- Black Hat hacker on the other hand can unethically exploit your system to make money out of it.

↳ Malwares are the programs written with malicious intent
↳ Malwares can include many things, such as:
- ~~Micro~~ Macro Viruses: viruses written in macro languages such as VBS. When a document is opened, they can run automatically.

Subject :

- Stealth Viruses: Hides the modifications it made & intercepts with the antivirus to provide false & bogus information to the operating system.
- Polymorphic Virus: Produces various copies of itself. It is difficult to detect.
- Self-garbling Virus: Attempts to hide from antivirus by modifying its code to not match predefined signatures.
- Bots & Zombies: Already compromised systems that have ability to exploit others.
- Worms can spread from one to another quickly.
- Rootkit are embedded in kernel & can exploit from there w/o getting detected.
- Firmware Rootkits hides in the firmware of your hardware and are worst of all.
- Key loggers & Trojans also exist. Trojans appear to be a useful thing but they are malware.
- Remote Access Tool (RAT) run on your system & allow others to remotely access your system.

★ Ransomware: Malware that has control of your PC & can covertly encrypt all of your files with a decryption key that only the hacker knows. Later they ask you for money to return the data.

★ Malvertisement: An online advertisement that is affected by a malware.

★ Spywares exist that gather information & send it to the Spy, the attacker. It is an intelligence gathering malware.

★ Adware forces advertisements on you. It falls under browser hijacking.

Subject :

PAGE NO.:
DATE:

★ Scareware is like a trap which tricks people to believe in a threat which isn't actually real.

## Phishing

↳ one of the most successful attack
↳ Cheap to setup
↳ Phishing happens when you give your information to a clone fake website that you believe, is authentic.
↳ fake emails are sent that contains the link to the fake site.
↳ Spear phishing is when you are targeted individually
↳ Techniques:
- Link Manipulation
  - ↳ Subdomains & Misspelt
  - ↳ IDN Homograph Attack (IDN: Internationalized Domain Name sta)
  - ↳ Hidden URLs

★ Real Domain: The domain name to the left of the HLD (High Level Domain) that has no / (back slash) to the left. (excludes https://)

Eg:

https://microsoft.com/info.html
is real but
https://stationx.net/micosoft.com/info.php
is not real

★ Vishing is phone or voice phishing.
★ SMShing is SMS phishing / text phishing.

★ Doxing: To do research on an individual or a company to find personal & private info.

Subject :

PAGE NO.
DATE:

* CPU Hijackers : take control of your CPU hardware to use it for mining crypto. Your device might be a crypto miner.
→ JavaScript based miners inject attack on a website you open & therefore the browser uses CPU to mine.
* To mitigate this, monitoring CPU usage is essential. You can also use adblockers to stop browser mining.

Darknet: A place that can be accessed only using special encryption or authorization. This is generally used for privacy, anonymity & to ensure security.
→ On the darknet, you might find many exploit kits & other illegal-to-share material on sale.