**Malicious Logic**

Malicious logic is a software, hardware, or firmware which is intentionally developed to attack systems. It’s capable of performing unauthorized action on a system which impacts its integrity and availability of its contents (information) and also violates the system’s security policy. Malicious logic comes in different ways like a **Trojan horse**, **Virus**, **Logic Bomb**, or a **Worm**. Malicious logic is also called Malware.

**Virus:**

Virus includes code to search for files to infect and it also makes copy of itself and attach itself to a file. A virus also relies on a host program to propagate from a system to another.

**Trojan:**

Trojan pretends to be a safe, helpful, or useful program but it contains unexpected functionality. Also a Trojan spread by some form of social media for ex. opening an email or a link or an advertisement and then the infection allows the attacker to access personal information.

**Worm:**

It looks similar to a virus which replicates itself but a Worm propagates copies of itself through a network. It’s also capable of seeking out new host systems which infects them.

**How to defend your system against a malware and detect it?**

Malware comes in different shapes and types and it’s really hard to detect it but there are some approaches that will help defending your system against these attacks.

1. Install an anti-virus and anti-malware, which will help in detecting viruses and malwares.
2. Remove unused communications ports, which will help in preventing the worm from propagating through the network.
3. Keep your system up-to-date with the security updates.
4. Use signature blocks to detect file alterations.
5. Detecting abnormal activities on networks.

**Malicious Logic Lesson (video):**

https://www.youtube.com/watch?v=wn-uVP8HncA