**Timeline of Cybersecurity Evolution**

The First Computer Virus (Creeper) was an experimental self-replicating program which was created by Bob Thomas in 1971.Although it was harmless, but it demonstrated the potential of self-propagating code, leading to the first antivirus program, Reaper.

The Term "Computer Virus" was Coinedby Fred Cohen which he introduced in the year 1983, while demonstrating how a program could replicate itself on a system.This led to a formal understanding of malicious software and the need for countermeasures.

Robert Tappan Morris released the Morris Worm in the year 1988, which infected 10% of the early internet.Ithighlighted the vulnerabilities of connected systems and led to the creation of the first Computer Emergency Response Team (CERT).

In the year 1990s, Firewalls and antivirus programs became standard security tools as malware threats increased. This marked the first widespread adoption of cybersecurity defences in businesses and personal computers.

In 2000, A fast-spreading email worm disguised as a love letter infected millions of computers. This demonstrated the risks of social engineering and the need for email security measures.

In 2010 Stuxnet (The First Cyberweapon), which is a highly sophisticated malware, was discovered targeting Iranian nuclear facilities.Thismarked the beginning of cyber warfare, showcasing how malware could cause real-world damage.

In 2013, there was a massive Data Breaches (Yahoo, Target, etc.)where by cybercriminals stole millions of records from major corporations.This raised awareness about data privacy, leading to stronger encryption and security regulations like GDPR.

In the 2020s an AI-Powered Cybersecurity & Zero Trust Model came into being where organizations began using AI to detect threats and adopted Zero Trust security models. This Improved real-time threat detection and emphasized continuous verification of users and devices.