**Name:** Bashar Tukur Shehu **Fellow ID**:FE/23/70792034 **Cohort:** Cohort 3

**Cyber Security Key Events from the earlier days of the internet**

|  |  |  |
| --- | --- | --- |
| Year | Event | Description |
| 1969 | Creation of **ARPANET by the Pentagon’s** Advanced Research Projects Agency. | Paving the way for more robust computer communication, greater vulnerability, and the eventual development of the Internet. |
| 1971 | Birth of Computer Virus/Worm - Creeper | Bob Thomas wrote a computer program that used PCs on the network to print the message: “**I’m the creeper; catch me if you can**.” |
| 1972 | Rise of the first Cyber Security program - Reaper | Ray Tomlinson developed Reaper, the first antivirus software, to chase and delete the Creeper virus on ARPANET. |
| 1983 | Creation of the standardized **TCP/IP protocol** which lead to the birth of the internet. | TCP/IP became the global standard for network communications, allowing networks all over the world to communicate easily with each other. |
| 1987 | Spread of **Vienna virus** | In the late 80s, the **Vienna virus** destroyed random files on computers it infected. A simple virus with many known variants... |
| 1987 | Rise of the first Antivirus program | Bernd Robert Fix created a program to neutralize the Vienna virus, making it the first known virus eliminated by an antivirus program. |
| 1988 | Internet Attack | Robert Morris, a Cornell graduate student, created the first Internet worm, which infected 10% of 60,000 computers online, causing significant damage. |
| 1990’s | Antivirus industry exploded | The rise of Windows in the early '90s led to increased viruses, prompting antivirus solutions like McAfee, Norton, and Kaspersky, which used signature-based detection. |
| 1999 | Mellisa Virus | David Smith's virus spread via Microsoft Outlook, sending emails titled "Important Message" with a malicious attachment that opened pornographic sites and disabled security features. |
| 2000 | ILOVEYOU Worm | The ILOVEYOU worm infected over 50 million computers by spreading via email, overwriting files, and auto-sending itself to Outlook contacts, forcing the Pentagon and CIA to shut down email systems. |
| 2001 | Fileless worm that evades antivirus detection | CodeRed exploited a buffer overflow to spread and launch DDoS attacks, evading traditional antivirus detection by operating as a fileless worm. |
| 2007 | Birth of iPhone – A computer in every pocket | Apple launched the iPhone, giving every user a pocket-sized, internet-connected computer more powerful than the computer that landed Apollo 11 on the moon. Smartphones constitute a significant cybersecurity concern because the sheer number of them vastly increases the potential attack surface for a hacker to exploit. |
| 2010 | First weaponized malware program | Stuxnet, the first globally weaponized malware, disrupted Iran’s nuclear program by sabotaging uranium centrifuges, marking a major cyber-espionage attack. |
| 2012 | Antivirus puts big data to work | Next-gen antivirus emerged as signature-based detection failed, using big data analysis to identify threats through user behavior, network traffic, and application activity. |
| 2013-1014 | Largest Data Breach in History | Yahoo’s massive breach exposed 3 billion user accounts, led to SEC fines and lawsuits, and remained undisclosed until 2016, marking a new era of large-scale cyberattacks. |
| 2020 | Rise of Connected Devices (IoT) | By 2020, an estimated 6.8 IoT devices per person increased cybersecurity risks as more personal data became exposed online. |

With each subsequent technological development, the tension between black-hat and white-hat hackers continues to grow. Both sides are quick to adapt their methods to try to catch the other unaware.

Today, cybersecurity is an intricate field, encompassing everything from endpoint security to network defenses, and now, Confidential Computing. The threats have become more sophisticated, leveraging AI and machine learning, making proactive and advanced defense mechanisms essential.