Decades of technological evolution has accelerated the reach and potential for distributed malware. A modern virus or worm can infect thousands of globally networked systems and cause millions in damage within minutes. The following list summarizes high-profile malware incidents over the past few decades.

**1988: Morris Internet Worm**

The father of Internet-born computer worms, Morris infected UNIX systems and became among the first to specifically target programming flaws to spread across networks. It also resulted in the first conviction under the 1986 Computer Fraud Abuse Act.

**1998: CIH Virus**

The CIH virus—named after Chen Ing Hau—caused an estimated minimum of $20 billion in damage worldwide and led to countless amounts of data being destroyed. CIH overwrote data on the host drive, including the basic input/output system (BIOS), causing severe damage.

**1999: Melissa**

Melissa makes the first noteworthy widespread appearance as a mass-mail Word macro virus that spread via contact lists to exploit trusted identities.

**2000: ILOVEYOU**

Ranks as the most rapid and widespread virus in history by e-mail attachment. Propagation also uses contact lists and exploits users through social engineering messages.

**2001: Code Red**

Code Red was a rapid Windows Internet Information Services (IIS) Web server infector that utilized victims as launch pads for attack. Code Red is notable for its rapid infection rate and use of short hit lists.

**2001: Nimda**

Nimda effectively spread in five different ways to target all versions of Windows. It spread via e-mail, open network shares, browser exploits, server exploits, and backdoors left by another virus.

**2003: SQL Slammer**

SQL Slammer is a tiny but rapidly spreading infector of Microsoft SQL servers. It transferred over user datagram protocol (UDP) packets and brought down high-profile financial systems.

**2004: MyDoom**

Originally spread via e-mail as a mechanism to turn victims into unwitting spam relays, it also migrated via peer-to-peer file sharing.

**2008: Conficker Worm**

A worm that targets Windows flaws and logins, Conficker grew large quickly to infect millions of systems across hundreds of countries. It was capable of automatic updates and self-armoring.