Hello! I'm here to help you with your question. Ransomware is a type of malicious software that has been around for several decades, and its history can be traced back to the early days of computer programming. Here's a brief summary:

1. Early beginnings (1980s-1990s): The first known instance of ransomware was created in the late 1980s by a group of hackers who went by the handle "The Dark Avenger." This early form of ransomware, called "AIDS Trojan," encrypted files on infected computers and demanded payment in exchange for the decryption key.
2. Emergence of commercial ransomware (mid-1990s): As the internet became more widely used, ransomware evolved into a commercial phenomenon. Cybercriminals began developing and selling ransomware tools, making it easier for individuals to launch attacks.
3. WannaCry and the global panic (2017): In May 2017, the WannaCry ransomware attack spread across 150 countries, infecting over 200,000 computers worldwide. This event brought ransomware to the forefront of cybersecurity concerns, leading many organizations to invest in prevention and response measures.
4. Development of new attack vectors (late 2010s): Attackers have continued to adapt their tactics, using newer methods such as phishing emails with malicious attachments or exploiting vulnerabilities in remote desktop protocols. These new attack vectors have made it increasingly difficult for organizations to keep pace with the evolving threat landscape.
5. Rise of double extortion (early 2020s): Double extortion refers to the practice of both encrypting and exfiltrating sensitive data from an organization's network. By holding both the encryption key and stolen data hostage, attackers can demand higher ransoms, making it harder for victims to recover their data without paying up.
6. Continued evolution and innovation (present day): As ransomware continues to evolve, so do the strategies and techniques used to combat it. Researchers and security professionals are working tirelessly to stay ahead of these threats, but the cat-and-mouse game between attackers

and defenders shows no signs of slowing down.

It's important to note that while this history lesson provides some context for understanding the nature and scope of ransomware, it cannot guarantee complete protection against future attacks. Stay vigilant, and always prioritize safety when dealing with unknown file extensions or suspicious email attachments!