Hello! I'm here to help you with any questions you may have. Ransomware has a complex and evolving history, so please bear with me as I provide a summary of its origins and development:

1. Early beginnings (late 80s-early 90s): The first known ransomware was the "AIDS Trojan," created in the late 1980s by a group of hackers in the Philippines. This malware would encrypt a victim's files and demand payment in exchange for the decryption key.
2. Emergence of the "encrypting ransomware" (mid-90s): As technology advanced, ransomware shifted from simply deleting or damaging files to encrypting them instead. This made it more difficult for victims to recover their data without paying the demanded ransom.
3. First major outbreaks (late 90s-early 2000s): In the mid-to-late 1990s, several high-profile ransomware attacks occurred, including the "I Love You" virus, which affected millions of users worldwide. These early attacks demonstrated the potential for ransomware to cause widespread disruption and highlighted the need for improved cybersecurity measures.
4. Growth and evolution (2000s-2010s): As ransomware became more sophisticated, attackers began targeting larger organizations and individuals. In 2013, the "CryptoLocker" strain emerged, which used advanced encryption techniques to make file recovery nearly impossible without paying the ransom. This period also saw the rise of "double extortion" tactics, where attackers stole sensitive data before encrypting it, doubling the pressure on victims to comply with demands.
5. Cybercrime marketplace growth (2010s): The underground market for buying and selling ransomware codes expanded, making it easier for less experienced criminals to purchase ready-made malware. This led to an increase in the number of ransomware attacks, particularly those using "wiper" malware that not only encrypted but also deleted files, causing permanent damage.
6. Wave of devastating attacks (2017-present): In recent years, there has been a surge in highly destructive ransomware attacks, such as WannaCry and NotPetya. These attacks have targeted critical infrastructure, leading to significant financial losses and reputational damage.
7. Evolution into "Big Game Hunting" (2010s-present): As ransomware continued to evolve, atta

ckers began focusing on large corporations and governments, often using social engineering tactics to gain initial access to systems. Once inside, they could spread the malware and encrypt valuable data, leading to multimillion-dollar payouts.

8. Modern ransomware trends (2020s): Recent years have seen a resurgence of older ransomware families, such as Locky and Bad Rabbit, as well as new variants like Maze and Sodin. These newer strains are often more sophisticated and harder to detect, allowing attackers to continue exploiting vulnerable targets.

Throughout this history, it is important to recognize that ransomware has become a significant threat to individuals, businesses, and governments alike. Understanding the evolution of these attacks can help us stay ahead of the game and protect ourselves against future threats.