Of course! I'd be happy to help you understand the history of ransomware.

Ransomware is a type of malicious software that has been around since the early 2000s. The first known incident of ransomware occurred in 2005, when the "WannaCry" worm infected computers across the world by exploiting a vulnerability in Windows operating systems. The attackers demanded payment in Bitcoin in exchange for unlocking the encrypted files.

Since then, ransomware attacks have become increasingly common and sophisticated. In 2013, the "GameOver Zeus" botnet was discovered, which used a complex network of infected computers to distribute ransomware to unsuspecting victims. The following year, the "CryptoLocker" strain emerged, which targeted Mac users as well as PC users.

In 2017, the "WannaCry" ransomware attack made global headlines after it infected over 200,000 computers in more than 150 countries, causing widespread disruption to healthcare services, transportation systems, and other critical infrastructure. The attackers demanded $300 worth of Bitcoin in exchange for unlocking the encrypted files.

The recent surge in ransomware attacks can be attributed to several factors, including:

1. The rise of cryptocurrency: The growing popularity of cryptocurrencies like Bitcoin has provided cybercriminals with an easy way to demand payments without leaving a trace.
2. The ease of distribution: With the advent of the internet and other digital technologies, it has become easier for cybercriminals to spread ransomware viruses through phishing emails, infected websites, or malicious ads.
3. The evolution of ransomware: Ransomware has evolved from simple encryption tools to more sophisticated programs that can evade detection and decryption.

4. The increase in online transactions: As more people conduct business online, there are more opportunities for cybercriminals to strike.

To protect yourself against ransomware, it's essential to practice good cybersecurity habits, such as:

1. Keeping your operating system and antivirus software up-to-date.
2. Backing up important data regularly.
3. Being cautious when opening emails or attachments from unknown sources.
4. Using strong passwords and avoiding clicking on suspicious links or downloads.

I hope this summary helps you understand the history and impact of ransomware. If you have any further questions, feel free to ask!