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 instance of ransomware was "AIDS Trojan," which surfaced in 1989 and infected over 15,000 computers worldwide. However, it wasn't until the late 2000s that ransomware became a more significant threat to computer users.

In 2006, a new strain of ransomware called "Ransom.Win32.CryptoLocker" emerged, causing widespread panic among cybersecurity experts. This particular variant encrypted files on infected systems, demanding payment in Bitcoin or other cryptocurrencies in exchange for the decryption keys.

Since then, ransomware attacks have only increased in frequency and severity. In 2017, the WannaCry ransomware attack affected over 200,000 computers across 150 countries, causing billions of dollars in damages. More recently, in 2020, a new strain of ransomware called "EKANS" targeted organizations in the United States, Europe, and Asia, highlighting the evolving nature of these types of attacks.

The evolution of ransomware has led to various tactics being employed by cybercriminals. These include:

1. Phishing emails: Cybercriminals use email campaigns to trick users into opening malicious attachments or clicking on links that download ransomware onto their devices.
2. Exploit kits: Attackers use exploit kits to take advantage of vulnerabilities in web browsers or plugins, allowing them to install ransomware on unsuspecting victims' machines.
3. Malvertising: Criminals use malicious ads to distribute ransomware through online advertising

networks.

4. Software vulnerabilities: Hackers identify unpatched software vulnerabilities and use them as entry points to deploy ransomware.
5. Insider threats: In some cases, ransomware can come from within an organization itself, with disgruntled employees intentionally spreading malware or exploiting vulnerabilities to hold data hostage.

It's important to note that ransomware attacks are not limited to individuals; they can also target large corporations, government agencies, and critical infrastructure providers. As such, it's crucial for all entities to stay vigilant against these types of cyberthreats and implement robust security measures to protect themselves.

I hope this summary provides you with a comprehensive understanding of the history of ransomware and its evolution over time. If you have any further questions or concerns, please don't hesitate to ask!