The History of Ransomware

Ransomware attacks have evolved significantly since they first emerged in the late 1980s. Here's a timeline of how this increasingly common cyberattack method has changed and developed over the past several decades:

1989: Ransomware Makes Its Debut

At this time, the first-ever ransomware attack was recorded. This incident — coined the AIDS trojan — was distributed via thousands of infected floppy disks at a World Health Organization conference for AIDS. After users inserted the compromised discs within their computers, their personal files were hidden, and a message appeared that demanded the victims send $189 (equivalent to $437 in 2022) to a P.O. Box in Panama to retrieve their files. However, this attack was shut down quite easily with file decryption technology.

1996: Experts Warn of Dangers to Come

While the 1990s passed by without any notable ransomware attacks occurring, computer scientists issued a warning in 1996 that more advanced forms of malware and data encryption were likely to emerge in the coming years — making ransomware a rising cyberthreat.

2005: Ransomware Sees an Uptick

During this time, ransomware incidents began to increase worldwide, often centered within Russia and Eastern Europe. This uptick can largely be attributed to a rise in the circulation of different ransomware variants, asymmetric encryption software and extortion methods. Nevertheless, these attacks were still relying on simple code, allowing most targets to deter such incidents with standard antivirus software. As a result, cybercriminals began transitioning to new attack vectors, such as phishing scams.

2009-2013: Cryptocurrency Creates Further Complications

Throughout this period, more advanced viruses and encryption software emerged (e.g., Vundo, WinLock, Reveton and CryptoLocker), compounding ransomware concerns. Additionally, the development of cryptocurrency (i.e., bitcoin) began permitting cybercriminals to obtain untraceable ransom payments, driving up overall ransomware activity.

SCS AGENCY INSURANCE

2015: Ransomware-as-a-Service (RaaS) Emerges

At this time, the RaaS model debuted. RaaS refers to a dark-web business model that permits sophisticated cybercriminals to sell their ransomware software to willing buyers, who then use it to launch attacks and secure ransom payments. This model has since allowed cybercriminals of any skill level to execute ransomware attacks, leading to a surge in incident frequency.

2018-Present Day: Incident Frequency and Severity Surges

Amid rising utilization of the RaaS model and the emergence of double and triple extortion techniques, ransomware incidents skyrocketed over the past few years. Today, large-scale attacks with major losses — such as WannaCry, Kasseya and Colonial Pipeline — have become all too common.

In this ever-changing cyber risk landscape, it's important now more than ever to take steps to address your unique ransomware exposures. Contact us today for the latest cybersecurity updates and solutions.