List of Famous Ransomware

WannaCry

- One of the most infamous ransomware attacks in recent years
- Targets vulnerabilities in Microsoft Windows operating systems
- Spread globally in May 2017

Ryuk

- Believed to have originated in Russia
- Targets businesses and organizations
- Uses encryption to lock victims' files in exchange for ransom

SamSam

- Targeted healthcare organizations, causing disruptions and millions of dollars in damages.
- Utilized bruteforce attacks to gain access to systems.
- Demanded payments ranging from $6,000 to $50,000 in Bitcoin.

Petya/NotPetya

- Named after the fictional Russian submarine from "The Hunt for Red October"
- Uses a worm to spread through networks
- Initially believed to be ransomware, later found to be a cyberattack disguised as ransomware

Cryptolocker

- First appeared in 2013
- Targets Windows devices
- Uses encryption to lock victims' files and demands payment in exchange for a decryption key

Locky

- Discovered in February 2016
- Spread through malicious email attachments
- Demands payment in Bitcoin

Maze

- First discovered in May 2019
- Targets businesses and organizations
- Threatens to leak sensitive data if the ransom is not paid

GandCrab

- Active from January 2018 to May 2019
- Discontinued by its creators after allegedly earning over $2 billion in ransom payments
- Spread through exploit kits and phishing emails

Sodinokibi/REvil

- Discovered in April 2019
- Believed to be linked to the Russian hacking group "GOLD SOUTHFIELD"
- Targets large corporations and demands large ransom payments

Bad Rabbit

- Hit Eastern Europe in 2017, spread through fake Adobe Flash installers on compromised websites.
- Encrypted files and demanded payment in Bitcoin.
- Used similar code to Petya ransomware.