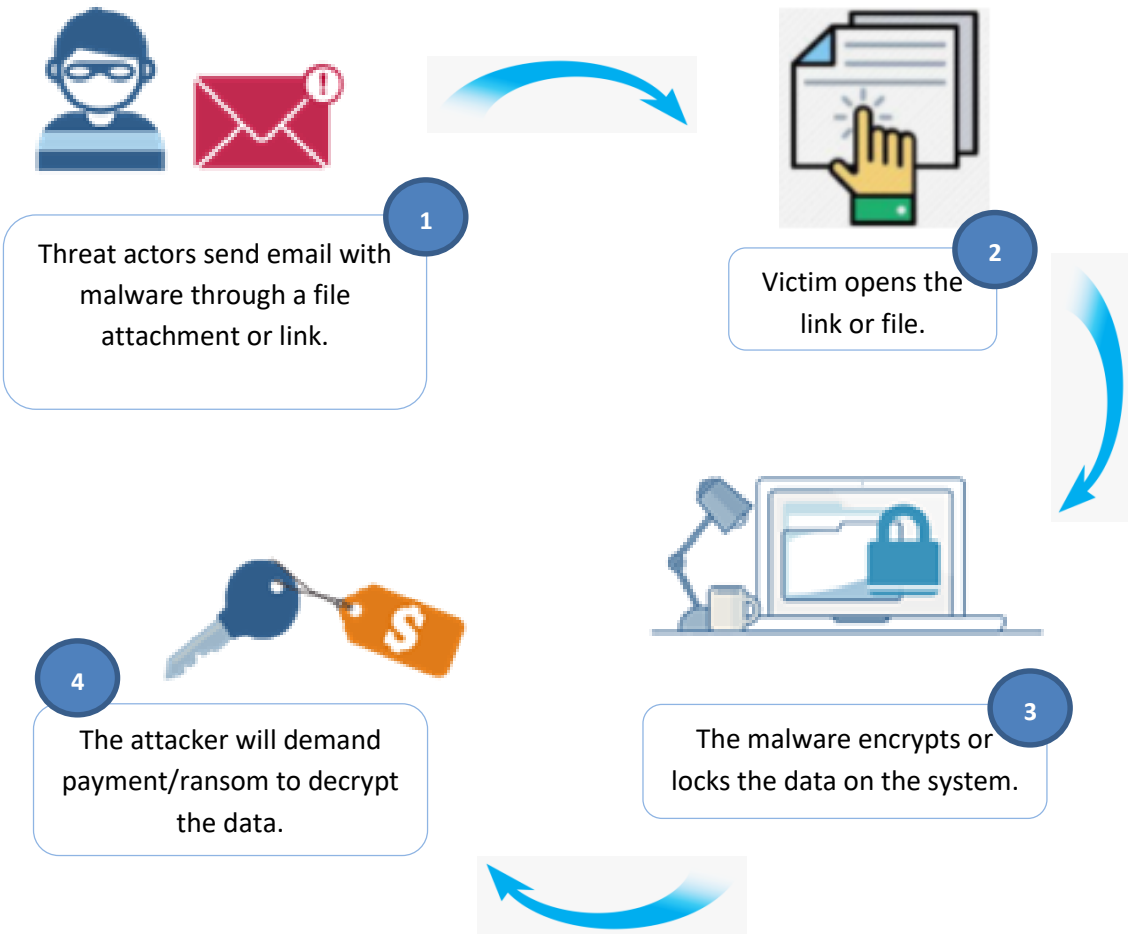
Ryuk Ransomware

Ryuk ransomware, pronounced as ree-yook, was first reported in mid-to-late 2018. Ryuk tops the list of the most dangerous ransomware attack and is accounted for three of the top 10 largest ransomware demands of the year. Russian cybercriminal group knows as Wizard Spider is known to be behind Ryuk ransomware and was also known for operating the Trickbot ransomware.

Ryuk is a type of crypto-ransomware that uses encryption to block access to a system, device, or file until a ransom is paid. Ryuk is often dropped on a system by other malware or gains access to a system via Remote Desktop Services. Ryuk demands payment and directs victims to deposit the ransom in a specific wallet. Once on a system, Ryuk will spread through the network using PsExec or Group Policy trying to infect as many endpoints and servers as possible. Then the malware will begin the encryption process, specifically targeting backups, and successfully encrypting them in most cases.

How it works



MITIGATIONS

- Invest in antimalware/antivirus protection.
- Ensure the system and all software is up to date.
- Back up data regularly.
- Educate yourself/employees on how to detect suspicious websites, emails and other scams.

REFERENCE

- https://us-cert.cisa.gov/ncas/alerts/aa20-302a
- https://www.malwarebytes.com/ryuk-ransomware