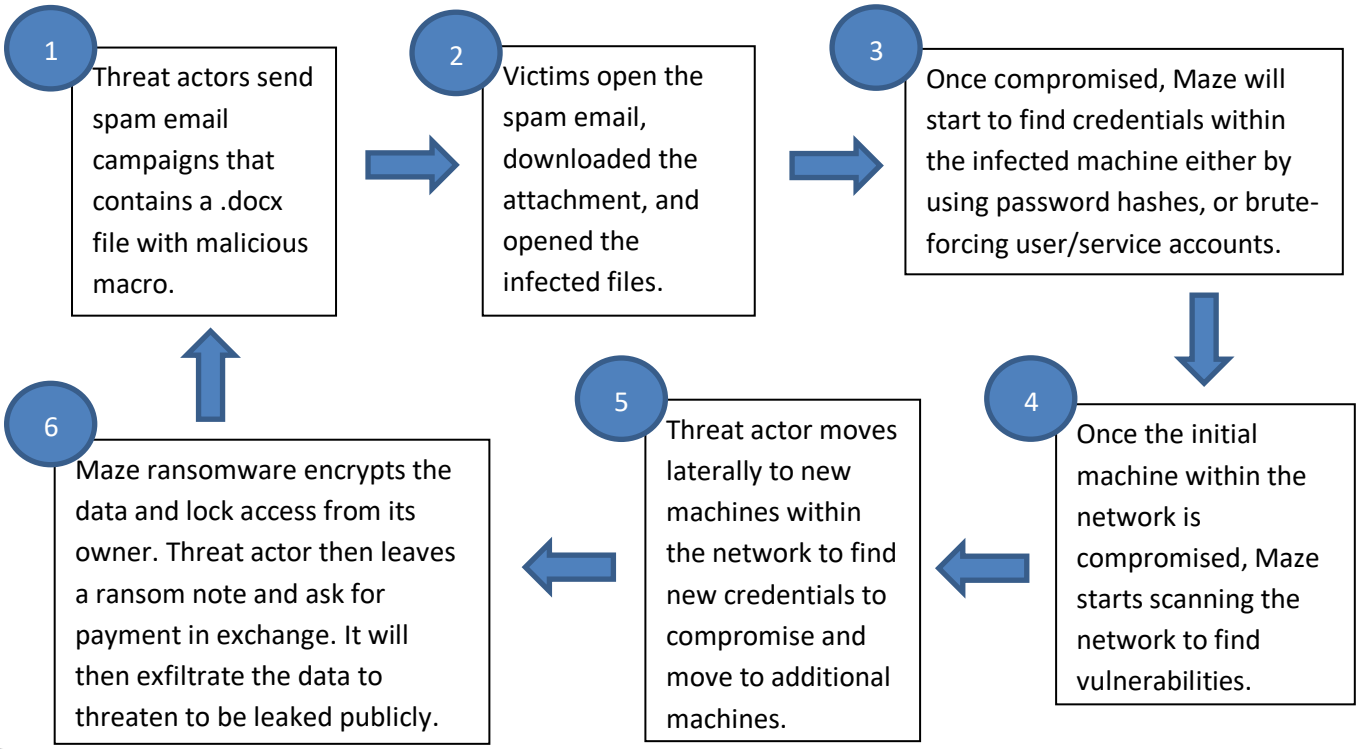
Maze Ransomware
(CSB21-01)

Maze ransomware, also known as "ChaCha" ransomware, was initially discovered in 2019 targeting organizations worldwide. The main goal of Maze ransomware is to encrypt all files and machines, and demand a ransom to recover the files.

Maze ransomware is usually distributed through exploit kits (Fallout EK and Spelevo EK), as well as email spam campaign with malicious attachments. Once the recipient opens the attached document, they will be prompted to enable editing mode wherein the malicious macro contained inside the document will run and will result to the victim's PC being infected with the ransomware.

Once infected, Maze ransomware will start exfiltrating all data within the infected computer and encrypt the machine, locking access from its users. Maze authors then leave a digital note to the victim letting them know that they need to pay ransom and on how to make the payment. If the victims refused to pay the ransom, Maze authors threaten that they will upload a copy of the stolen data as proof of penetration.

HOW IT WORKS



IMPACT

- Infects computer with ransomware that will encrypt victim's files and machine blocking owner's access to the infected computer.
- Threat actors steal documents and threatens victim that they will publish a copy of the stolen data on the internet if the ransom was not paid.

MITIGATIONS

- Monitor and audit network traffic for any suspicious behaviors or anomalies;
- Keep all software, systems and applications patched and up to date;
- Use multi-factor authentication (MFA) to add extra layer of security;
- Avoid suspicious emails and links;
- Review any software carefully before downloading;
- Use strong, unique passwords;
- Install anti-virus/anti-malware software and ensure it is updated;
- Regularly conduct anti-virus scanning on your computer and network;
- Always keep a backup copy of files to reduce impact of ransomware; and
- Increase awareness of how ransomware spreads i.e. through spammed emails and attachments.

REFERENCE

- https://www.mcafee.com/blogs/other-blogs/mcafee-labs/ransomware-maze/
- https://www.csa.gov.sg/singcert/publications/rising-prominence-of-maze-ransomware