DSCI
PROMOTING DATA PROTECTION
A NASSCOM® Initiative

MAZE RANSOMWARE

NASSCOM-DSCI ADVISORY

'Maze' Ransomware Attack

A leading global IT service provider, confirmed on 18th April that a security incident involving its internal system led to some disruption, as the result of a Maze ransomware attack. As a responsible industry player, the company has not only informed its clients but also reported the incident to the relevant government authorities. Security teams of the company, with the help of experts, are actively taking steps to contain this incident. It has also engaged with law enforcement authorities on the matter.

The Indian industry takes such incidents seriously. At an individual level, companies take all desired precautions, deploy forward-leaning measures, and monitor diligently. Indian IT industry is aware of rising attacks globally in the backdrop of COVID-19 outbreak. The industry has joined NASSCOM and DSCI's efforts for creating a collective response to security challenges through sharing of the learnings and best practices.

The Maze ransomware attack is an example of advancing malware that tends to move laterally in the network and has the potential to cause disruptions and information stealing for extortion, as per the information available. Since the COVID-19 outbreak, Maze ransomware is targeting companies across sectors, including Healthcare, IT/ITeS and Banking across the globe. It supposedly gets delivered via emails having attachment embedded with macros to encrypt files using sophisticated techniques. NASSCOM and DSCI advise caution and vigilance against such attack family. Based on the learnings and information available, we recommend:

- Block exploit kits that are distributed via malicious advertising. Maze ransomware uses Fallout, and Spelevo exploit kits
- Strengthen email security to detect harmful attachments
- Ensure that the environment doesn't run unsigned macros
- Conduct regular phishing awareness campaign to alert the users and contain the spread of spammed emails and attachments
- Lockdown Remote Desktop Protocol, if not in use or follow RDP best practices such as rate limiting, 2FA, etc.
- Deploy effective backup strategies including keeping the backup safe
- Ensure segmentations of the network to limit the spread
- Ensure patching, secure configuration, frequent assessment, and vigilant monitoring of remote access granting systems
- Follow best practices for granting system permissions to the files

NASSCOM and DSCI advise referring to the advisories issued by government authorities, such as CERTs. For the benefit of our members, we have also published a technical report.

Read the Maze Technical Analysis Report