Maze Ransomware and its Various Campaigns Continue to Threaten the Cyber World

A brief description of the Maze ransomware campaigns and activities.

Ever since this year began, the Maze ransomware has been hitting headlines. Recently researchers discovered more samples of Maze in numerous industries making it one of the major threats for the cyber-world.

Maze ransomware initially tries to get a strong idea of the target device's internal surroundings and begins to create a place for itself. Once that's done it tries to access user privileges to carry lateral movements and kick start the file encryption throughout drives. But, before the encryption, files are exfiltrated so as to be used for future compulsion in any way possible.

If the security system of a device isn't laden with necessary protective gauges it could possibly crash completely under the pressure of Maze ransomware. The infection could put sensitive information at large and incapacitate operations almost killing the company's finances.

According to a report, there's an "Anti-Ransomware Protection module" which hunts ransomware related encryption-based activities. It allows users to keep track of the activities.

Per sources, lately, Maze ransomware was spotted compromising several IT service providers. It also set up a footing in another victim device's network via insecure Remote Desktop Protocol or by using brute-force on the account of the local administrator. Cloud backups too aren't safe from the Maze ransomware because they are widely tracked on the vulnerable networks. With the login credentials, all backed-up data could be sent to the threat-actors via a server under their control.

The solution for any such occurrences is as repetitive as ever; stronger security mechanisms, better passwords especially remote systems with remote access possibilities and of course, heftier protection measures.

Maze Ransomware: What you need to know and How to protect from being hit by Maze!

Maze encrypts the system and steal the data thus it's not just a malware attack but a fusion of ransomware attack and data breach.

Cognizant Technology Solutions Corp., an IT giant with 3000 employees was recently hit by a strain of sophisticated Windows Ransomware called Maze, encrypting its systems and threatening to make its data public if they don't pay the supposed ransom.

This particular malware is proving to be quite lethal and is making headlines every week with their new victim. It has spread quite a disarray and chaos not only in the IT sector but even in other companies and firms which deal with sensitive user data.

It attacked Andrew Agencies in October then the city of Pensacola, US Insurance Company Chubb, the leading cable manufacturer Southwire Company (America), Medical Diagnostic Laboratories (MDLabs), Manitoba Law Firm (Canada) and now Cognizant.

How is it more Different and Lethal than other Ransomware?

There have been other malware that encrypt files and demand ransom but what makes Maze more dangerous is that it encrypts the system and steal the data and export it to hackers or threaten to release it on their own website (yes, they have a website where they publish their new victim and their data) if the ransom is not paid thus it's not just a malware attack but a fusion of ransomware attack and data breach.

https://www.ehackingnews.com/2020/05/maze-ransomware-and-its-various.html

https://www.ehackingnews.com/2020/04/maze-ransomware-what-you-need-to-know.html