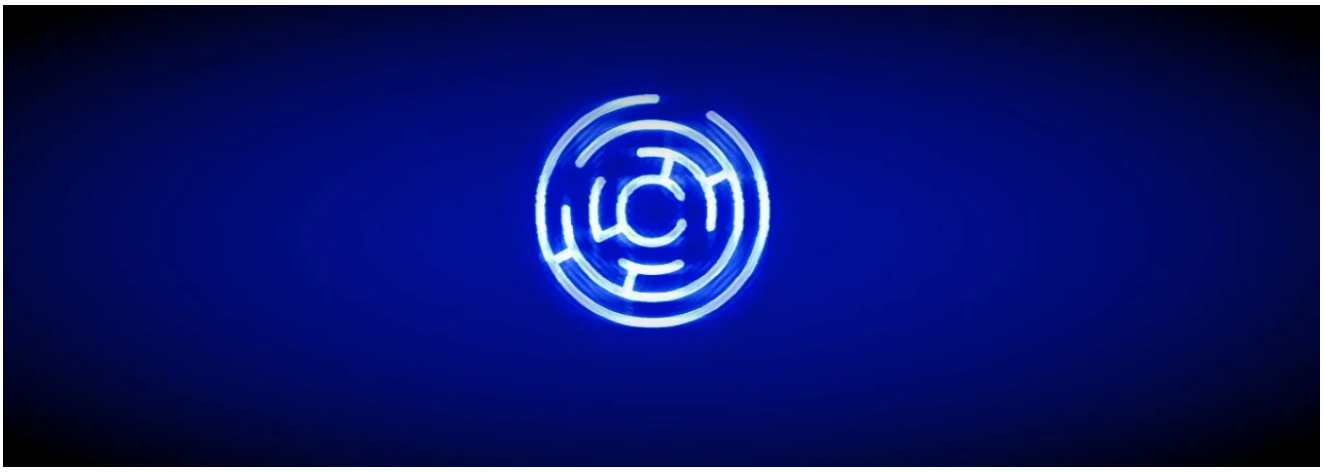
IT services giant Cognizant suffers Maze Ransomware cyber attack

bleepingcomputer.com/news/security/it-services-giant-cognizant-suffers-maze-ransomware-cyber-attack/

Lawrence Abrams

By
Lawrence Abrams

- April 18, 2020
- 01:45 PM
- 1



Information technologies services giant Cognizant suffered a cyber attack Friday night allegedly by the operators of the Maze Ransomware, BleepingComputer has learned.

Cognizant is one of the largest IT managed services company in the world with close to 300,000 employees and over $15 billion in revenue.

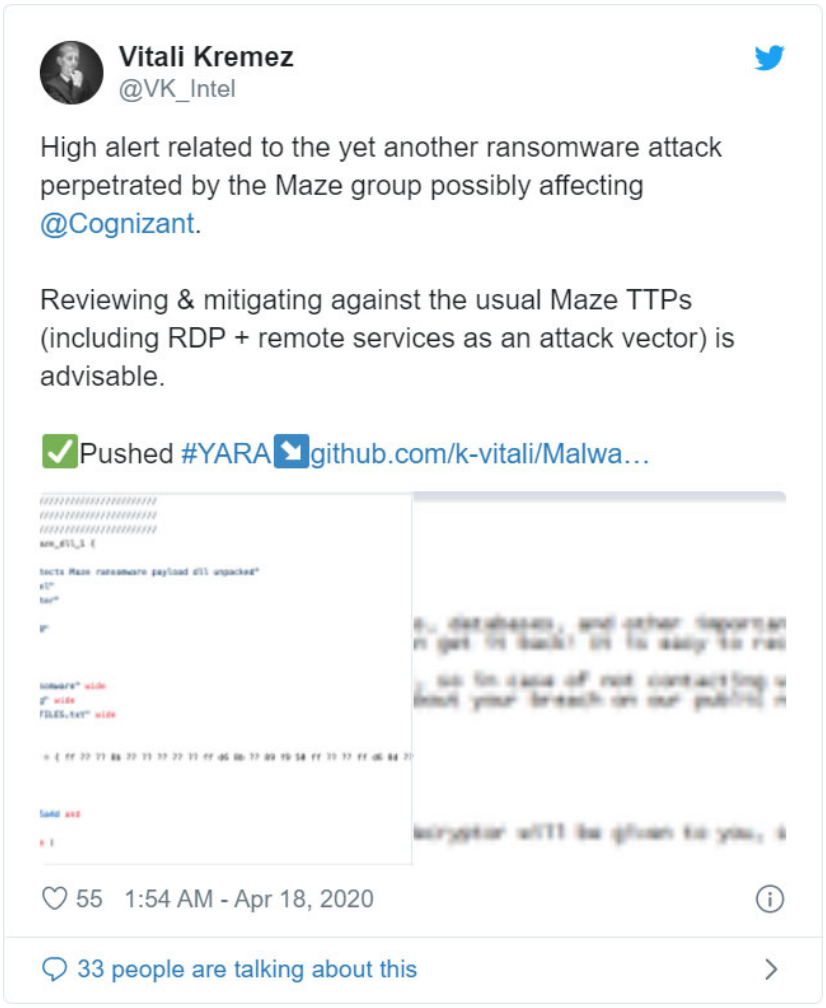
As part of its operations, Cognizant remotely manages its clients through end-point clients, or agents, that are installed on customer's workstations to push out patches, software updates, and perform remote support services.

On Friday, Cognizant began emailing their clients, stating that they had been compromised and included a "preliminary list of indicators of compromise identified through our investigation." Clients could then use this information to monitor their systems and further secure them.

The listed IOCs included IP addresses of servers and file hashes for the kepstl32.dll, memes.tmp, and maze.dll files. These IP addresses and files are known to be used in previous attacks by the Maze ransomware actors.

There was also a hash for a new unnamed file, but there is no further information about it.

Security research Vitali Kremez has released a Yara rule that can be used to detect the Maze Ransomware DLL.



When we contacted the Maze operators about this attack, they deny being responsible.

In the past, Maze has been reticent to discuss attacks or victims until negotiations stall. As this attack is very recent, Maze is likely not discussing it to avoid complications in what they hope would be potential ransom payment.

After reporting on this attack, Cognizant posted a statement to their web site that confirms the cyber attack was by Maze Ransomware:

Cognizant can confirm that a security incident involving our internal systems, and causing service disruptions for some of our clients, is the result of a Maze ransomware attack.

Our internal security teams, supplemented by leading cyber defense firms, are actively taking steps to contain this incident. Cognizant has also engaged with the appropriate law enforcement authorities.

We are in ongoing communication with our clients and have provided them with Indicators of Compromise (IOCs) and other technical information of a defensive nature.

Threat actors were likely on the network for weeks

If the Maze operators conducted this attack, they were likely present in Cognizant's network for weeks, if not longer.

When enterprise-targeting ransomware operators breach a network, they will slowly and stealthily spread laterally throughout the system as they steal files and steal credentials.

Once the attackers gain administrator credentials on the network, they will then deploy the ransomware using tools like PowerShell Empire.

If it was Maze, it must be treated as a data breach

Before deploying ransomware, the Maze operators always steal unencrypted files before encrypting them.

These files are then used as further leverage to have the victim pay the ransom as Maze will threaten to release the data if a victim does not pay.

Chubb info on Maze news site

These are not idle threats as Maze has created a "News' site that is used to publish stolen data from non-paying victims.

If Maze was not behind the attack as they claim, there is still a good chance that data was stolen as that has become a standard tactic used by ransomware operators.

For this reason, all ransomware attacks must be treated as data breaches.

This is a developing story.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.