Written by Marco Attard
24 April 2020

Service provider Cognizant is the latest victim of Maze, a particularly virulent strain of malware that has interrupted parts of Cognizant business as it affects internal systems and "some" customers.

The company is a giant in the field, and counts big names such as ING, Standard Life and Mitsubishi Motors as clients. So far it has not disclosed the names of clients potentially affected by the attack, but does say it may lead to revenue loss and incremental costs. The group associated with Maze denies involvement with the attack, but security experts do not dismiss Maze from responsibility.

“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,” a statement from the company reads. “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.”

Like other ransomware, Maze encrypts the data on infected Windows machines, but it does so with a twist. It also forwards copies of the data to the attackers for a spot of extra leverage. After all, if the ransom is not paid the attackers can simply sell off the confidential corporate data. As mentioned earlier, the Maze group denies responsibility of the attack, but monitoring service Under the Breach reports it spotted someone selling access to a "major IT provider" a week before the attack. Thus, one can speculate another hacker cracked into Cognizant before providing the Maze group with an open door.

Maze was involved in a number of high-profile ransomware attacks since it was discovered in May 2019, and has lead to lawsuits, email impersonation attempts and trolling efforts. It historically relies on exploit kits, remote desktop connections with weak passwords and email impersonation, as well as an exploit involving a Flash Player use-after-free vulnerability. January 2020 saw the release of a Maze update, one featuring text poking fun at security researchers. It states “without malware, your [sic] work will be boring as hell, what will you cover? I know you hate us, but you need to know that we love you researchers, without you our job also would be f****** boring as hell.”

Go Cognizant Security Incident Update