Cybersecurity Capstone Breach Response - Case Study

Company	Cognizant
Breach Type	Ransomware
Strain	Maze Ransomware

Context

Cognizant

Cognizant is an American multinational information technology services and consulting company. It is headquartered in Teaneck, New Jersey, U.S. Cognizant is part of the NASDAQ-100 and trades under CTSH. It was founded as an in-house technology unit of Dun & Bradstreet in 1994, and started serving external clients in 1996.

Like many other IT services firms, Cognizant follows a global delivery model based on offshore software R&D and offshore outsourcing. The company has a number of offshore development centers outside the United States and near-shore centers in the U.S., Europe and South America.

Cognizant is organized into several verticals and horizontal units. The vertical units focus on specific industries such as Banking & Financial Services, Insurance, Healthcare, Manufacturing and Retail. The horizontal units focus on specific technologies or process areas such as Analytics, mobile computing, BPO and Testing. Both horizontal and vertical units have business consultants, who form the organization-wide Cognizant Consulting team together. Cognizant is among the largest recruiters of MBAs in the industry; they are involved in business development and business analysis for IT services projects

[source: wikipedia]

Maze Ransomware

Maze is a strain of ransomware that has been impacting organizations since 2019. Although one main group created Maze, multiple attackers have used Maze for extortion purposes. In addition to encrypting data, most operators of Maze also copy the data they encrypt and threaten to leak it unless the ransom is paid.

A Maze ransomware infection combines the negative effects of ransomware (lost data, reduced productivity) with those of a data breach (data leaks, privacy violations), making it of particular concern for businesses.

Modus Operandi

When Maze ransomware first came into use, it was mostly distributed through malicious email attachments. More recent attacks use other methods to compromise a network before dropping the ransomware payload. For instance, many Maze ransomware attacks have used stolen or guessed **Remote Desktop Protocol (RDP)** credentials (username and password combinations) to infiltrate a network. Other attacks have started by compromising a **vulnerable virtual private network (VPN)** server.

Once Maze is inside a network, it takes the following steps:

1. **Reconnaissance**: Maze investigates the vulnerabilities of the network and identifies as many connected machines as possible, helping to ensure the eventual ransomware activation has maximum impact. The reconnaissance process is usually completed several days after attackers infiltrate the targeted network.
2. **Lateral movement**: Maze uses the information it gained during reconnaissance to spread itself across the network, infecting as many devices as possible.

3. **Privilege escalation**: As Maze moves laterally, it steals more credentials, enabling it to spread to additional machines. Eventually it usually acquires administrator credentials, which give it control over the entire network.
4. **Persistence**: Maze uses a number of techniques to resist removal. For example, it may install backdoors (hidden ways around security measures) into the network so it can be re-installed if it is discovered and removed.
5. **Attack**: Finally, Maze begins the process of encrypting and exfiltrating data. Once data has been encrypted, Maze displays or sends a ransom note telling the victim how to make payment, unlock their data, and prevent a data leak.

Timeline

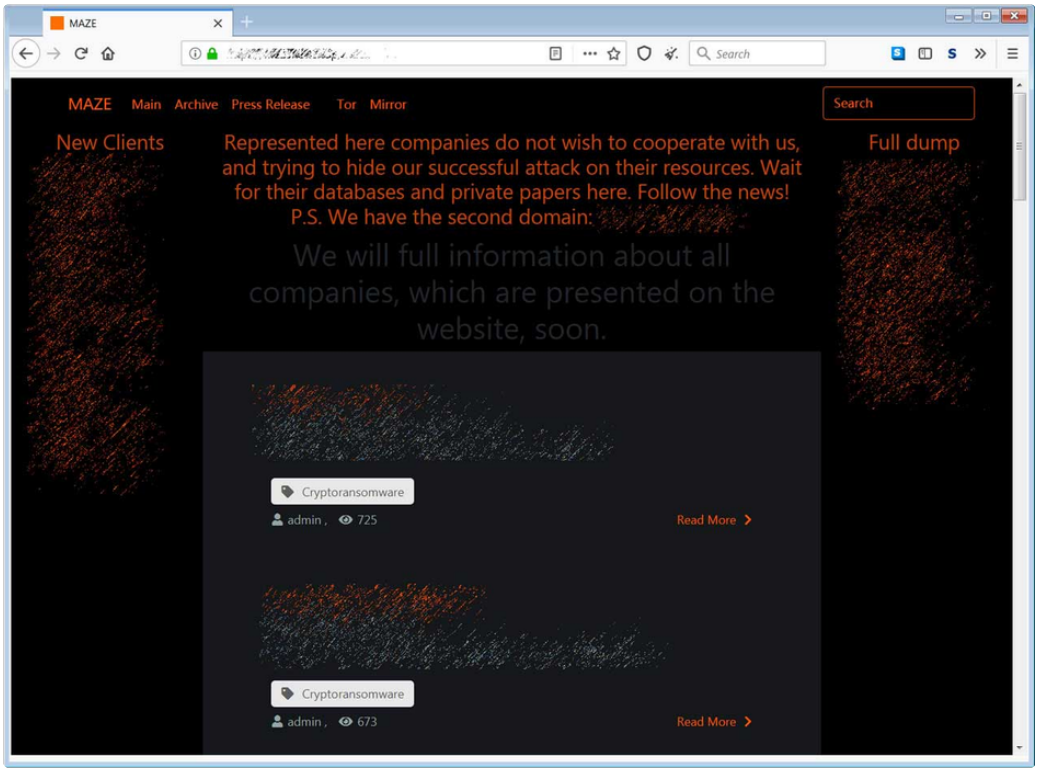
On April 17th, 2020, Cognizant suffered a ransomware attack, with data being exfiltrated, exposing information about its users. According to Cognizant CEO Brian Humphries, the incident only impacted its internal network, but not customer systems. More precisely, Humphries said the ransomware incident impacted Cognizant's select system supporting employees' work from home setups and the provisioning of laptops that Cognizant was using to support its work from home capabilities during the COVID-19 pandemic.

After the company was aware of the attack, some service were shut down to prevent further exploits.

In two data breach notification letters filed with the Office of the Attorney General of California, Cognizant states that the Maze Ransomware operators were active on Cognizant's network between April 9th and the 11th.

During the time they had access, they "likely exfiltrated a limited amount of data from Cognizant's systems."

Before deploying ransomware and encrypting devices, the Maze Ransomware operators will first spread laterally through the network and steal unencrypted files.



Maze Ransomware

In the data breach notifications, Cognizant warned sensitive personal information such as SSN, Tax IDs, financial information, and driver's licenses, and passports may have been stolen.

> ⚠ "We have determined that the personal information involved in this incident included your name and one or more of: your Social Security number and/or other tax identification number, financial account information, driver's license information, and/or passport

information," the Cognizant customer data breach notification stated.

For employees who have corporate credit cards, Cognizant warned that they were likely exposed during the attack.

> ⚠ "The majority of the personal information that was impacted was information relating to our corporate credit cards. Out of an abundance of caution, we are giving notice to all associates who have an active corporate credit card. All associates who have an active corporate credit card will be offered credit and identity theft monitoring services from ID Experts"

Costs

- Cognizant estimates the loss from the cyberattack to be between 50 - 70 million dollars.
- The Chief Financial Officer stated there will be some unpredicted expenses due to the attack: legal counsel. consulting, and other expenses regarding the investigation, disaster recovery and remediation of the data breach.

Prevention

- Data encryption needs to be implemented on files with sensitive data.
- Investment on employee training and education.
- Build a robust remote work infrastructure of managed devices.
- Strong passwords and multi-factor authentication should be implemented.
- Constantly apply patches to workstations and servers.
- Backup data regularly and securely.
- Secure RDP connections and Citrix servers.

References

Cognizant

What is Maze ransomware? | Cloudflare

Cognizant expects to lose between $50m and $70m following ransomware attack

IT giant Cognizant confirms data breach after ransomware attack