Ransomware - Cognizant

- On April 17th, 2020, Cognizant suffered a ransomware attack.

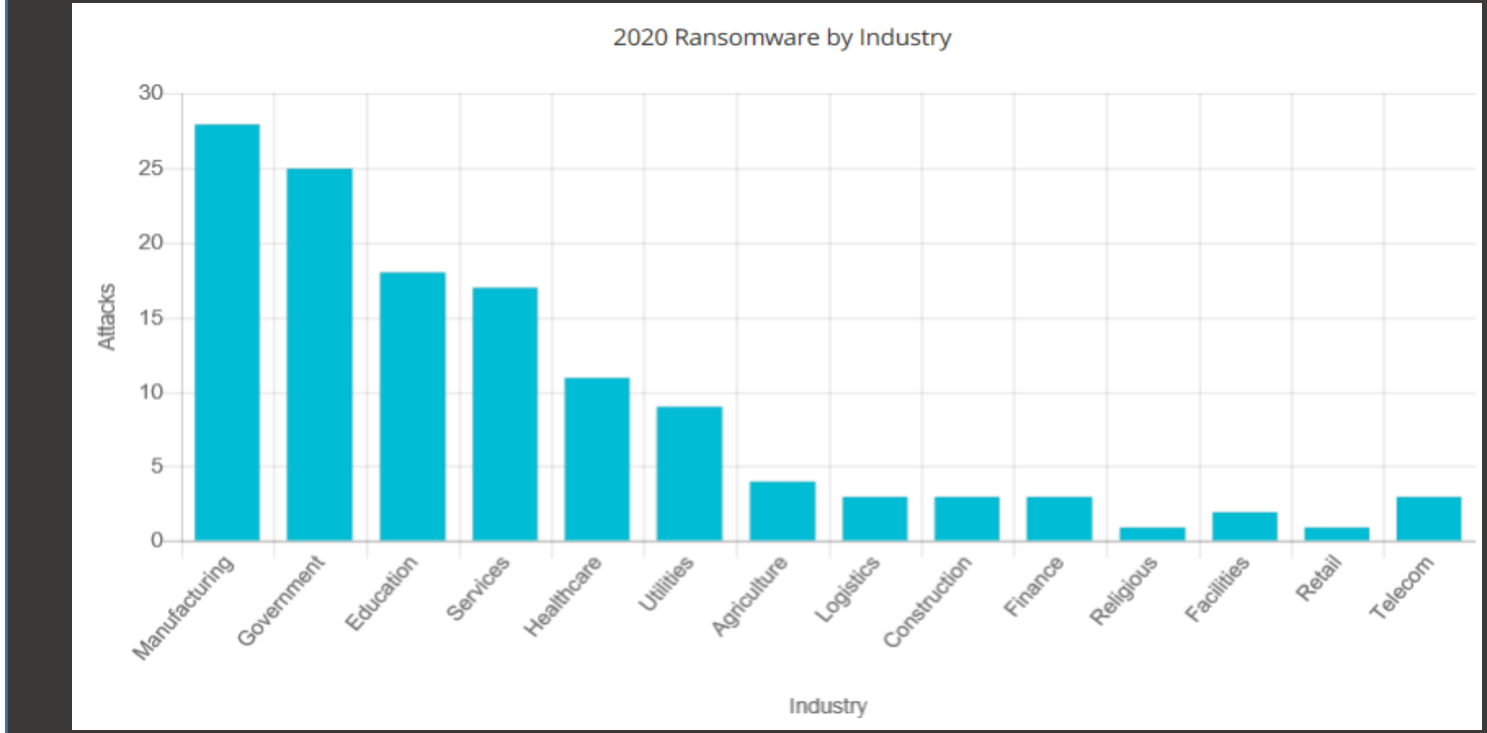
- Cognizant, one of the biggest IT managed services company, suffered from a data breach, exposing information from its users.

- The virus used to attack the company was a Maze Ransomware.

Maze Ransomware attack

Like other ransomware attacks, Maze can spread through a company´s network by infecting systems and encrypting data in order to deny access.

Moreover, a Maze Ransomware is more threatening because it also steals the data it finds and exfiltrates it to the hackers´ servers. Hackers then ask for a payment to give the data back and threat the company to make the data public or put it for sale if the ransom is not paid.



Cognizant

YOUR FILES ARE ENCRYPTED
Your photos, documents and other important files have been encrypted with unique key, generated for this computer.
NEXT

- Cognizant is a United States based company that provides global IT services; such as digital, technology, consulting, and operations services. Its headquarters is located on Teaneck, New Jersey.

- The Ransomware attack affected the company´s internal systems, causing issues for some of its global clients.

- The ransomware incident impacted:
  - Cognizant's system setup supporting employees telework
  - The company´s laptops that were being used for the telework capabilities during the COVID-19 pandemic.

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

Timeline

1. April 17th, 2020: Cognizant, the giant IT managed services company, suffered from a Ransomware cyberattack.

2. Cognizant announced that the hackers from the Ransomware attack accessed its network between April 9th and the 11th.

3. On May 11th, Cognizant's CEO stated that the company has recovered completely from the attack and most of its services are back to operation.

4. Cognizant shares had decreased by 13% this year due to the virus pandemic and cyberattack

Vulnerabilities

Unencrypted data

When the hackers had access to the network, they exfiltrated a limited amount of data from Cognizant’s system.

Server vulnerability

A security vulnerability was found on the Citrix server that runs Cognizant’s Trizetto healthcare solutions system.

Costs

- Cognizant estimates the loss from the cyberattack to be in the range of $50 to $70 million.
- The Chief Financial Officer stated that there will also be some unpredicted expenses due to the attack; involving legal, consulting, and other expenses regarding the investigation, service restoration, 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.

References

- Lawrence, Abrams (2020, June 17th) IT giant Cognizant confirms data breach after ransomware attack. Retrieved from https://www.bleepingcomputer.com/news/security/it-giant-cognizant-confirms-data-breach-after-ransomware-attack/

- No Author (2020, May 11th) Cognizant Anticipates $50-70 Million Loss Following Ransomware Attack. Retrieved from https://www.securitymagazine.com/articles/92361-cognizant-anticipates-50-70-million-loss-following-ransomware-attack

- Balaji, N (2020, June 19th) Cognizant Confirms Data Breach Following Ransomware Attack. Retrieved from https://cybersecuritynews.com/cognizant-data-breach/

- Zitter, Leah (2020, April 24th) Incident of the Week: Cognizant Attacked by Maze Retrieved from https://www.cshub.com/attacks/articles/incident-of-the-week-cognizant-attacked-by-maze

- Hope, Alicia (2020, May 13th) Maze Ransomware Attack on Cognizant May Impact Customers. Retrieved from https://www.cpomagazine.com/cyber-security/maze-ransomware-attack-on-cognizant-may-impact-customers/