Cognizant Maze Ransomware Attack Explained using Diamond Model

Siddharth Madikeri[1]

[1]School of Cybersecurity and Privacy, Georgia Institute of Technology

November 30, 2022

Abstract

The diamond model describes cyber attacks by underlining the characteristics and relationships of four components- adversary, capability, infrastructure and victim. This paper will discuss the 2020 Maze ransomware attack on Cognizant. The model will give a better understanding of the extent of the attack and the risks it posed to the organization. This paper will also give a policy assessment on how the imminent threat of ransomware attacks can be addressed.

Keywords

Ransomware, Adversary, Cyberspace, Cybercriminal, Personal Identifiable Information (PII)

1 INTRODUCTION

One of the most dangerous and prevalent threats to cyberspace is ransomware.[9] It is a type of malware which encrypts a target victim's confidential data where the adversary demands a payment, or "ransom", in order to restore access to the data. The effects of ransomware can cost companies millions due to damage. In 2020, the average ransomware payment was around $233,817 and now, in 2022, it has risen to $925,162. This is excluding downtime, remediation and damage expenses.

Maze ransomware,[8] previously known as "ChaCha ransomware", has targeted organizations across the world. It comes in the form of a strain, spread out through spam emails and exploit kits demanding large amounts of money in return for the recovery and decryption of stolen data. Maze is an affiliate-based ransomware that operates through a network of developers that share the profit with different groups that infiltrate into corporate networks.

The incident reviewed in this paper is about the Maze ransomware attack on Cognizant. Companies like Cognizant are not well-positioned to protect their stakeholder data because, for them, a good Cybersecurity strategy is expensive. They are required to produce profits for their shareholders as their main goal, and Cybersecurity is just an afterthought.

2 BACKGROUND

Cognizant, a Fortune 500 company, became a victim of the vicious Maze ransomware attack in April 2020. Employees could not communicate with each other or with customers due to the deletion of internal directories caused by the attack. The fact that the employees had to work remotely during the COVID-19 pandemic, made it even more challenging. The company needed to take help from cybersecurity experts and their internal IT security teams to destabilize the situation.

The inventors of Maze ransomware, the Maze Gang,[3] created a malicious tactic called "double extortion", where the victim is threatened with a leak of their compromised confidential data if they refuse to co-operate and pay the ransom. In addition to shutting down network access for employees, the malware creates a replica of the entire network data and uses it to lure the company into meeting the ransomware demands.[10]

The Maze ransomware has affected many people - employees of large organizations, their investors, and customers whose data was held hostage by the Maze Gang. Southwire, a cable and wire manufacturer and a victim of the ransomware, had a $6 million ransom demanded,[7] while another unnamed organization had $15 million demanded.[3] Cognizant estimated a $50-$70 million loss due to the attack. This included the ransom payment, legal expenses, investigation services, and remediation costs.[1] Many of the company's customers revoked access to their networks, and so, Cognizant could not service those customers for some time.

3 DIAMOND MODEL

This section will describe the four categories of the diamond model along with its two axes - Social-Political and Technology. These two features will

give a better understanding of the attack between the sections of the model.

3.1 Adversary

The adversary operator and customer are the same in this case - the Maze Gang. They are an anonymous group of underground cybercriminals. The intent of the attack was financial, as they held the victim's data for ransom money under the threat of extortion.

3.2 Victim

The victim was Cognizant, an American multinational IT services and consultancy company, currently with 341,000 employees and revenue of $16.8 billion in 2019. The company is a worldwide operation with customers spread across the globe. They disclosed the Maze ransomware incident to the public on April 18, 2020.[2]

3.3 Capability

The Maze Gang utilized their custom-developed Maze ransomware to its many capabilities. They have triggered the installation of Maze using the techniques of spam and spear-phishing with Microsoft Word documents. Multiple victims have identified the use of RATs (Remote Access Trojans) and Cobalt Strike Beacons. Exploit kits including Fallout EK and Spelevo EK were used to gain initial access to victim networks.[6] PowerShell scripts have been used to transfer confidential data via FTP. The malware's command and control (C2) channel was hosted with the help of different IP addresses. The Gang has made use of Meterpreter agents and Cobalt Strike Beacons, which indicates that the C2 infrastructure contains a Cobalt Strike server and a Metasploit server.

3.4 Infrastructure

Maze's infrastructure contained an FTP server for the purpose of data exfiltration. C2 channel callbacks have been found to be from different sources reaching out to many Russian or Lithuanian IP addresses in the following ranges - 91.218.114.11/30, 91.218.114.12/30, 91.218.114.16/31, 91.218.114.24/29. Several domains like aoacugmutagkwctu[.]onion, mazedecrypt[.]top, mazenews[.]top and newsmaze[.]top were used by the Gang to publicly post data of victims that refused to pay the demanded ransom. One of the domain names was first registered with Namecheap, an ICANN-accredited domain name registrar based in Los Angeles, and was hosted on a server leased from World Hosting Farm Ltd., an Ireland-based firm.[4]

3.5 Social-Political meta-feature

Cognizant, the victim organization, was attacked by the Maze Gang, which is a group of cybercriminals. They had provided the adversary with employee and customer personal identifiable information (PII). The attackers' intent was financial, with the purpose of espionage and extortion. They stole the victim's confidential data, encrypted all the file systems, and extorted the victim for money, while threatening to release the data to the public. The cost to Cognizant for not paying the ransom would have been private data disclosure, which would be a huge hit to the company, and its investors and clients. It cost the company millions to bolster their cybersecurity strategy.

3.6 Technology meta-feature

The capabilities of the malware were executed using the infrastructure. Known tools used for the attack included Cobalt Strike's Beacon (RAT), Mimikatz (a tool used for stealing credentials), Meterpreter (RAT), Bloodhound (a tool used for mapping the shortest path to a domain administrator) and PowerSploit/PowerView (Invoke-ShareFinder) for reconnaissance, PowerShell scripts for downloads and file exfiltration via FTP, and batch scripts for the deployment of the Maze ransomware in Window's domains.[6] Once the malware is installed, data is encrypted, and a ransom message is left in the file "DECRYPT-FILES.txt", which is present in every possible directory.[5] The file would contain instructions on how to pay the ransom along with a threat to disclose the confidential data if demands were not met.

The fact that Cognizant did not have the controls to detect the activities before confidential data shows how neglectful they were with respect to their cybersecurity operation. They could have prevented, or at least detected, many malicious precursor activities if they had good enough security controls in place.

4 POLICY ASSESSMENT

Ransomware attacks, like Maze, are a nationwide problem and they are not specific to a particular company, so they should be handled at the National level (layer 9). Since citizens' private data is very important to protect, civil rights at the national level is the best approach. Data breaches cause immense damage not only to the organization involved, but also to the customers who trust the organization. National laws should mention the forceful protection of customer data for any organization storing that data. Many organizations, like Cognizant, do not defend customer data even with adequate security measures, which tells us that there is a market failure for cybersecurity. The likelihood of becoming a victim to any breach is unknown and

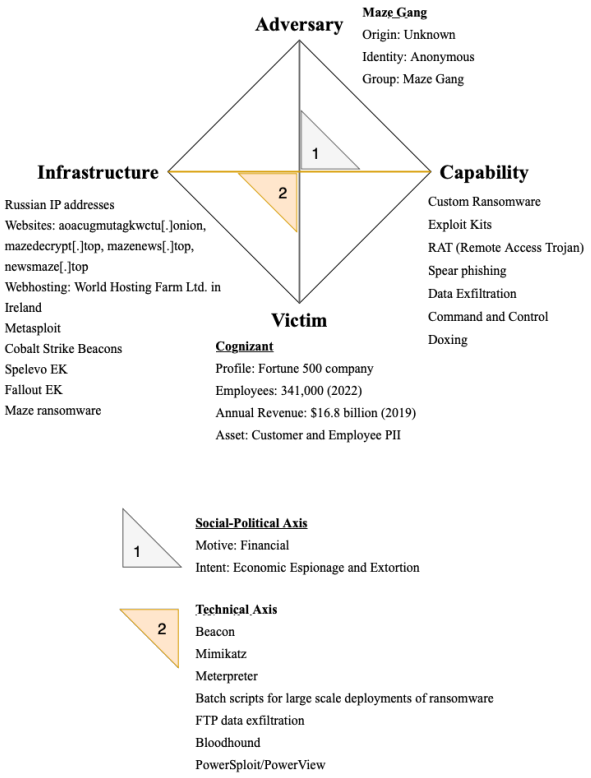

Figure 1: Diamond model of the Cognizant Maze Ransomware attack

cannot be predicted. But looking at any organization's perspective, without specific risk details and expensive security tools and personnel, it can be discouraging to install protection to secure customer data appropriately. If it is up to the organization, the decision for securing data is cost analysis. Almost every company is profit-driven, so there would be a conflict between reducing expenses to increase profits and spending money on security controls.

To combat ransomware attacks, policy changes to implement updates and patches are necessary. There must be a ransomware policy at the national level stating basic controls and requirements each organization should have. In addition to this, each organization should have a separate ransomware policy containing detailed procedures related to preventing, monitoring, responding to and recovering from a ransomware incident. Popular strategies that could have helped stop Maze attacks include enforcing application whitelisting, patching applications and security flaws, configuring Microsoft Office macro settings, employing application hardening, restricting administrative privileges, patching operating systems and implementing multi-factor authentication.

5 CONCLUSION

In this paper, we analyzed the Maze ransomware attack on Cognizant using the diamond model, describing each component of the incident. Even though the Maze Gang has retired,[3] Maze-like ransomware will always be prevalent, and ransom will continue to be paid by companies and their stakeholders until a National action is taken. In addition to passing a law, a compliance agency should be introduced to make sure each organization is following that compliance. A law is likely the only way to force all companies to protect customer and citizen PII sufficiently.

References

[1] Cognizant expects to lose between $50m and $70m following ransomware attack. https://www.zdnet.com/article/cognizant-expects-to-lose-between-50m-and-70m-following-ransomware-attack/.

[2] IT services company Cognizant warns customers after 'Maze' ransomware attack. https://www.computerweekly.com/news/252481865/IT-services-company-Cognizant-warns-customers-after-Maze-ransomware-attack.

[3] Maze, a notorious ransomware group, says it's shutting down. https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/.

[4] Maze Ransomware Victim Sues Anonymous Attackers. https://www.bankinfosecurity.com/maze-ransomware-victim-sues-anonymous-attackers-a-13574.

[5] Maze Ransomware Update: Extorting and Exposing Victims. https://www.sentinelone.com/labs/maze-ransomware-update-extorting-and-exposing-victims/.

[6] Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents. https://www.mandiant.com/resources/blog/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.

[7] Ransomware victim Southwire sues Maze operators. https://www.darkreading.com/threat-intelligence/ransomware-victim-southwire-sues-maze-operators.

[8] What is Maze ransomware? Definition and explanation. https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware.

[9] What is Ransomware? https://www.crowdstrike.com/cybersecurity-101/ransomware/.

[10] What you need to know about the Cognizant maze ransomware attack. https://www.makeuseof.com/know-about-cognizant-maze-ransomware/.