Applying the Diamond Model to Cognizant (MSP) vs. Maze Ransomware

By Killbit

Published: 2024-06-22 · Archived: 2026-04-10 03:01:01 UTC

11 min read

Dec 14, 2020

Introduction

In our modern era, one of the most prevalent threats to the computing world is ransomware. Ransomware is a form of malware that, once executed, encrypts files and the victim's attached network shares (Columbus, 2019). Once the files and connected network shares have become encrypted, the victim is presented with a ransom note that generally states for a payment to be made in exchange for the private key to decrypt the victim's data. This attack is crippling to victim organizations that need access to their files and data to maintain daily operations. The disruptions from ransomware can cost companies millions in damages. The average ransomware payment is about $233,817, with the median cost of $110,532. Maze malware makes up 13.6% of the ransomware market share, landing it in second place among top strands (Siegel 2020). It is estimated that ransomware caused $7.5 billion in damages last year in the United States (O'Neill 2019). A research group at Emisoft tallied up 113 governments and agencies, 764 health-care providers, and up to 1,233 individual schools affected by ransomware in America (O'Neill 2019).

The incident reviewed in this paper is about the Maze ransomware attack on a Fortune 500 organization. The organization under attack was Cognizant, which was among the largest of the Maze ransomware victims. Maze ransomware was initially discovered in May of 2019 by Jerome Segura, a researcher at Malwarebytes (Cybersecurity and HHS Cybersecurity Program 2020). Maze ransomware many initial access methods, post-exploitation methods, and data exfiltration techniques before encrypting victim data. The Maze ransomware operation is unique as it was the first notable version to add the element of extortion for enforcement of the demanded ransom payment (Arntz 2020).

Companies like Cognizant are not well-positioned to protect their customer and employee data because, for them, a robust Cybersecurity strategy is a cost-driven choice versus a legal requirement. Corporations are required to produce profits for their shareholders as their primary mission, where Cybersecurity is an afterthought. Without a dis-incentive for non-compliance, there is no way to ensure that citizen PII will be secured appropriately.

History of the problem

The history of the ransomware problem is prevalent and ever-present, however prosaic. The first significant strain of modern ransomware came into the forefront of the Cybersecurity industry in 2013 and was dubbed "CryptoLocker" (Kieran 2020). CyrptoLocker's behavior was to use 2048-bit RSA encryption on all files for which it had access permissions under the context of the compromised user account. In the process of encrypting files, the file names were simultaneously changed to have extensions such as ".cryptolocker" (Petters 2020). A text file would be left on the desktop titled "DECRYPT_INSTRUCTION," containing steps toward recovering the victim's data (Petters 2020). Victims would be instructed to transfer some amount of bitcoin to a digital wallet controlled by the attacker(s) in exchange for the encryption key to decrypt their data (Kieran 2020). After the CyptoLocker campaign's success, which earned more than $3 million, many new strains and variants of ransomware were released by the criminal underground (Groot 2020).

Ransomware variants ran into many problems when it came to receiving payments. At times there were difficulties collecting payment due to attackers failing to keep their side of the deal (Hartwig 2016). Attacker reputations would be ruined after not following through with their side of the transaction. Attackers that did not issue the decryption key in exchange for the ransom discouraged future victims from bothering to make ransom payments. Large corporations also implemented proper backup solutions to revert to a previous backup without making the ransom payment. Also, they deployed cyber defense tools to not only detect but, in some cases, prevent the malware from running. At a certain point, researchers released tools for free called "decryptors" that decrypt victim files without paying the attackers.

The ransomware industry in 2019 produced an estimated 7.5 billion in revenues (Hartwig 2020). Trends seem to suggest the market will grow to 20 billion by 2021 (Cook 2020). Many ransomware variants have been reverse-engineered. The reverse-engineered code has been publicly posted on GitHub for anyone to study. One can only speculate that with the news and source code of many ransomware variants publicly available, Maze developers found a way to refine their malware to achieve tremendous financial success. Maze, unlike its predecessors, added the elements of exfiltration and extortion (Arntz 2020). The exfiltration of plaintext data allowed the group to blackmail their victims into paying the ransom demanded under the threat of releasing the private data publicly. This extortion tactic paid dividends as it removed the option for non-payment as the cost of non-payment may ruin the victim organization's reputation beyond repair.

Extent of the problem

The Maze ransomware variant affected many people. The people involved include large corporations, the employees of those large corporations, their investors, and the citizens whose data became the product consumed by the Maze Gang. Public news announced that one victim corporation was known as Southwire, a wire and cable manufacturer, had a 6-million-dollar ransom demanded (Sheridan 2020) while another anonymous company had 15 million demanded (Whittaker 2020). Cognizant estimates a $50 — $70 million loss as the attack has them paying a ransom, investigation services, legal expenses, restoration, and remediation costs (Cimpanu 2020). Cognizant's investors have likely been startled, causing expected investment losses, which are probably figured into the estimation, as the corporate entity is publicly traded in the stock exchange. Many customers of Cognizant have revoked access to their networks (Javier 2020); thus, Cognizant cannot, at least temporarily, service those customers.

Applying the Diamond Model

Adversary

The adversary operator and adversary customer, in this case, are the same, the Maze Gang. The Maze Gang is an anonymous underground criminal operation. The adversary has developed a well-known form of ransomware coined, “Maze Ransomware.” The adversary’s intent is financial as they hold victim data for ransom money under threat of extortion.

Victim

Cognizant is a Fortune 500 Managed Service Provider with 283,100 employees and revenue of $16.8 billion in 2019 as touted by cognizant.com. Cognizant is a worldwide operation with customers all over the globe. Cognizant publicly disclosed their Maze ransomware incident on April 18, 2020 (Culafi 2020).

Capability

The Maze Gang has many capabilities, including their custom-developed advanced Maze ransomware. They have exercised spam and spear-phishing coupled with Microsoft Word documents containing malicious macros to trigger the installation of their Maze ransomware. The use of remote access trojan, Cobalt Strike Beacons, have been identified across multiple victims. The use of exploit kits, including Fallout EK and Spelevo EK, have been used to gain initial footholds on victim networks (Kennelly 2020). PowerShell scripts have been used to transfer victim data via FTP. The Maze Gang has published collected victim records on their website http://mazenews[.]top. The Gang’s command and control were hosted behind many IP addresses; many were Lithuanian and Russian, as can be referenced in this paper’s Infrastructure section. The Maze Gang has shown to use Cobalt Strike Beacons and Meterpreter agents, which indicate that the C2 infrastructure at a minimum contains a Metasploit server and a Cobalt Strike server.

Infrastructure

The Maze infrastructure contains an FTP server for data exfiltration purposes. Command and control callbacks have been witnessed by many sources reaching out to many Russian IP addresses included in the following ranges: 91.218.114.11/32, 91.218.114.12/30, 91.218.114.16/29, and 91.218.114.24/31 (Kennelly 2020). These addresses may be nothing more than proxies and a tactic to misdirect researchers or deter law enforcement agencies. The Gang controls several domains as well, including mazenews[.]top, newsmaze[.]top, and mazedecrypt[.]top (Kennelly 2020), where the group publicly posted data of victims that did not pay the ransom (Schwartz 2020). These domains were active in Ireland, running web servers within World Hosting Farm Limited, which inadvertently hosted the Maze Operation’s web front (Schwartz 2020).

Technology Meta-Feature

Cybersecurity research groups have discovered technologies frequently paired with Maze ransomware. Known precursors to Maze ransomware include the use of Meterpreter (RAT), Cobalt Strike’s Beacon (RAT), Mimikatz (a tool frequented to steal credentials), Bloodhound (for mapping the shortest path to domain administrator), encoded

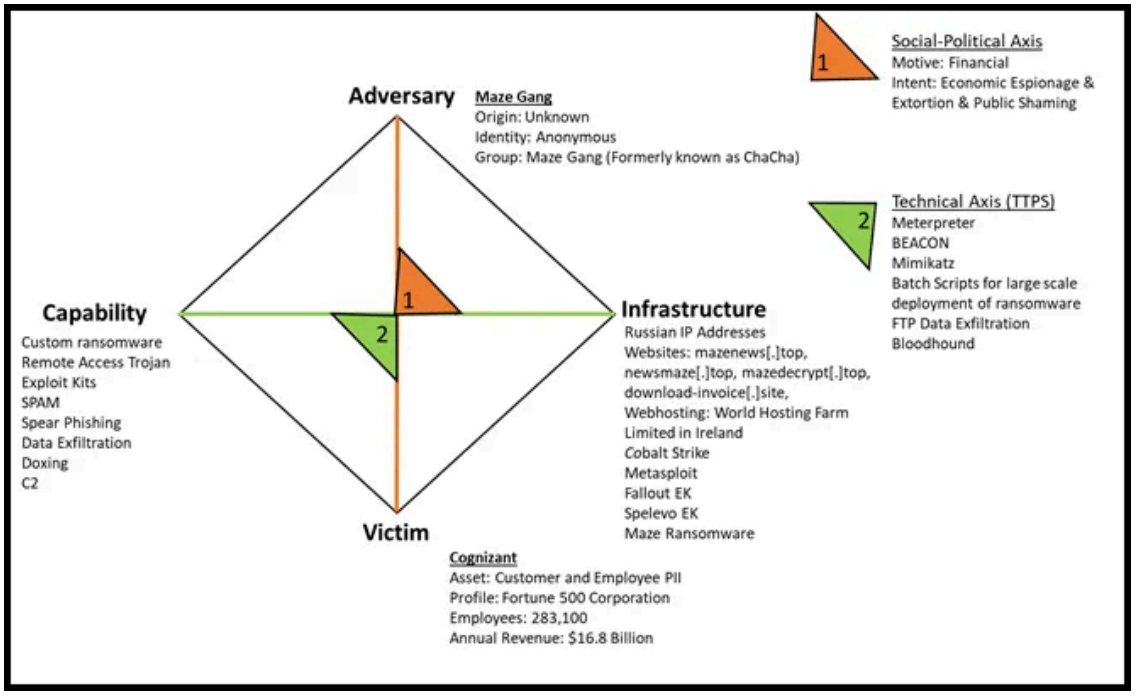
PowerShell scripts executed for malicious downloads as well as FTP file exfiltration, and batch scripts for large scale deployment of the Maze ransomware across a Window's domain (Kennelly 2020). Once the precursor activities have been completed and the Maze ransomware is installed, critical data is encrypted, and a ransom letter is left in every directory possible with the file name "DECRYPT-FILES.txt" (Walter 2020). The ransom letter contains instructions on how to pay the ransom along with a threat to release stolen data publicly if payment is not received.

These attack tools are ubiquitous for both white hat hackers known as Penetration Testers and Red Team Operators for legitimate testing purposes. As such, creating indicators of compromise in defensive toolings such as Intrusion Detection Systems, Advanced Endpoint Threat Detection tools, and even antivirus solutions are relatively trivial and, in most cases, already exist. The fact that Cognizant did not detect the activity before losing customer and employee PII is a testament to how neglectful they have been with their internal Cybersecurity operation expenditures. Suppose Cognizant (and other victims) had proper security in place, IoCs could have been implemented to detect or even prevent many malicious precursor activities; thus, they could have actively booted the attackers off their network(s).

Social-Political Meta-Feature

The victim organization in this campaign provided the adversary the product of customer and employee personally identifiable information (PII). The adversary's intent was financially motivated with the purpose of economic espionage, extortion, and public shaming. The adversary pulled off a "smash and grab" operation. They stole the victim's valuable data, encrypted their file systems, and proceeded to extort the victim for money, threatening to release the data publicly. The approach establishes the adversary as non-persistent and can be marked as "Fleeting" on the persistence spectrum. The extortion technique prevents the victim from simply restoring their systems from backups to avoid the ransom. Cognizant could have chosen not to pay the ransom. The cost to Cognizant would then have been private data public disclosure, which would have scarred its identity, and its clients as well as investors' confidence. Thus, breaking these trust relationships would ultimately lead to losing current and future customers and current and future investments in the organization.

Diamond Model Diagram



Policy Assessment

To best address the imminent threat of ransomware attacks such as Maze, it would be best approached from a policy perspective of layer 9, the national layer. The problem is a Nationwide issue and is not specific to any single organization, so it should be handled at the National level. The national-level civil rights approach is best because citizen data privacy is of the utmost importance. Any organization that wants to have the privilege of storing valuable private citizen data should also be forced to protect it heavily. Market failure for Cyber Security is prevalent where many organizations, including Cognizant, do not adequately defend customer data. When organizations face the cost of securing customer data, the incentives are low. The price of a data breach is difficult to quantify. The likelihood of becoming a victim is equally a mystery to most organizations. The cost-benefit analysis to justify expenditures on expensive experienced Cyber Security personnel and costly security tooling is often non-existent. Without specific risk details and given such a high cost of defensive measures, it is easy to see how this strongly discourages organizations from readily adopting protections to secure citizen and customer data appropriately. While some publicly disclosed meta-level reports do come out sporadically from various sources concerning the cost of Cyber breaches, it appears that decision-makers at the organizational level can’t help but have some degree of cognitive dissonance. In other words, “Why should our organization bare the cost of these security measures when it is possible that we are never attacked?” Many organizations have the misconception that they can use legal action to threaten attackers and intimidate them, thus thwarting attacks and data leaks. Other organizations believe they can set aside enough money to account for losses as an operational expense that can then be mitigated by purchasing Cyber Liability insurance alone. When left to the organization, the decision for securing citizen data is a cost analysis. When under a profit-driven capitalist economic model, an inherent conflict exists between reducing expenses to raise profits and data security’s optional expense.

Conclusion

Companies do not adopt healthy security postures to protect their customer and employee data because it is a sizeable and currently optional expense — the evolution of ransomware trending towards Ransomware-as-a-Service (Keijzer 2020, 106–108) virtually guarantees that it will continue to propagate at alarming rates. The extensive cost of Maze-like ransomware will continue to be paid by corporations, stockholders, employees, and citizens until National layer action is taken. The Diamond model analysis provided laid out the components of the incident. If the government operating at the national societal layer passed a law to enforce compliance with minimum data security standards concerning citizen data, this would remove the inter-organizational struggle to justify the cost and force it to become a cost of doing business-specific nation. In addition to putting a law in place, a third-party compliance agency or agencies should be established to certify each organization's compliance. A law is likely the only way to force all industries to protect citizen and customer data sufficiently. Without a dis-incentive for non-compliance, there is no way to ensure that citizen PII will be secured appropriately.

If you like my content and the work I have provided here please consider sending some coffee love my way @ https://www.buymeacoffee.com/killbit

References

3/29/2020, Jeff Petters Updated: 2020. "CryptoLocker: Everything You Need to Know." *Inside Out Security*. March 30. https://www.varonis.com/blog/cryptolocker/.

6/19/2020, Kieran Laffan Updated: 2020. "A Brief History of Ransomware." *Inside Out Security*. June 20. https://www.varonis.com/blog/a-brief-history-of-ransomware/.

Arntz, Pieter. 2020. "Maze: the Ransomware That Introduced an Extra Twist." *Malwarebytes Labs*. May 28. https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/.

Cimpanu, Catalin. 2020. "Cognizant Expects to Lose between $50m and $70m Following Ransomware Attack." *ZDNet*. ZDNet. May 8. https://www.zdnet.com/article/cognizant-expects-to-lose-between-50m-and-70m-following-ransomware-attack/.

Columbus, Louis. 2019. "Shadow IT Is The Cybersecurity Threat That Keeps Giving All Year Long." *Forbes*. Forbes Magazine. December 15. https://www.forbes.com/sites/louiscolumbus/2019/12/15/shadow-it-is-the-cybersecurity-threat-that-keeps-giving-all-year-long/?sh=10d90c8e5561.

Cook, Sam. 2020. "50+ Ransomware Statistics & Facts for 2018–2020." *Comparitech*. November 16. https://www.comparitech.com/antivirus/ransomware-statistics/.

Culafi, Alexander. 2020. "Cognizant Discloses Maze Ransomware Attack." *SearchSecurity*. TechTarget. April 20. https://searchsecurity.techtarget.com/news/252481892/Cognizant-discloses-Maze-ransomware-attack.

Groot, Juliana De. 2020. "A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time." *Digital Guardian*. October 6. https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

Hartwig, Chris. 2016. “Ransomware Variant Won’t Decrypt Files After Ransom Paid.” *WatchPoint Security Blog*. July 27. https://blog.getcryptostopper.com/ransomware-variant-wont-decrypt-files-after-ransom-paid.

Cybersecurity, and HHS Cybersecurity Program. 2020. *Maze Ransomware*. Vol. 202006041030. Washington DC, VA: HHS.

Javier, Rozelle Alyssa. 2020. “Cyber Insurers Brace for Payout after Cognizant Breach — Insurance Insider.” *Cyber Insurers Brace for Payout after Cognizant Breach — Insurance Insider | S&P Global Market Intelligence*. July 14. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/cyber-insurers-brace-for-payout-after-cognizant-breach-8211-insurance-insider-59413789.

Keijzer, Noel. 2020. “The New Generation of Ransomware — An in Depth Study of Ransomware-as-a-Service.” *University of Twente*. June 25. http://essay.utwente.nl/81595/1/Keijzer_MA_EEMCS.pdf.

Kennelly, Jeremy. 2020. “Navigating the MAZE: Tactics, Techniques and Procedures Associated With MAZE Ransomware Incidents.” *FireEye*. May 7. https://www.fireeye.com/blog/threat-research/2020/05/tactics-techniques-procedures-associated-with-maze-ransomware-incidents.html.

O’Neill, Patrick Howell. 2020. “Ransomware May Have Cost the US More than $7.5 Billion in 2019.” *MIT Technology Review*. MIT Technology Review. April 2. https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019.

Schwartz, Mathew J. 2020. “Maze Ransomware Victim Sues Anonymous Attackers.” *Bank Cybersecurity*. January 3. https://www.bankinfosecurity.com/maze-ransomware-victim-sues-anonymous-attackers-a-13574.

Sheridan, Kelly. 2020. “Ransomware Victim Southwire Sues Maze Operators.” *Dark Reading*. Dark Reading. January 3. https://www.darkreading.com/threat-intelligence/ransomware-victim-southwire-sues-maze-operators/d/d-id/1336719.

Siegel, Bill. 2020. “Q3 Ransomware Demands Rise: Maze Sunsets & Ryuk Returns.” *Coveware*. Coveware: Ransomware Recovery First Responders. November 4. https://www.coveware.com/blog/q3-2020-ransomware-marketplace-report.

Walter, Jim. 2020. “Maze Ransomware Update: Extorting and Exposing Victims.” *SentinelLabs*. August 6. https://labs.sentinelone.com/maze-ransomware-update-extorting-and-exposing-victims/.

Whittaker, Zack. 2020. “Maze, a Notorious Ransomware Group, Says It’s Shutting Down.” *TechCrunch*. TechCrunch. November 2. https://techcrunch.com/2020/11/02/maze-ransomware-group-shutting-down/.
