A CASE STUDY

ON

RANSOMWARE ATTACKS IN CYBER SECURITY

By

Girish Pareek

05th Aug 2020

Maze Ransomware Attack

Abstraction.

IT managed services firm Cognizant suffered a ransomware by Maze ransomware found recently on April 17, 2020. Cognizant is one of the biggest IT managed services companies in the world who has shared a preliminary list of indicators (IoC) of compromise identified after their investigation to assist their clients to help them monitor their system and further secure them.

Introduction.

Maze ransomware was first discovered by a Malwarebytes security researcher Jerome Segura on 29 May 2019. This ransomware was earlier known as ChaCha ransomware. The main objective of Maze ransomware is to encrypt all files it can in an infected system and then demand a ransom to recover those files. However, the important characteristic of Maze is that the ransomware authors threaten to release the victim's information on the internet if they do not pay.

During this attack on Cognizant, Maze got distributed by the Fallout exploit kit through a fake site, which was pretending to be a cryptocurrency exchange app.
Attackers created a fake cryptocurrency site to help them purchase traffic from ad networks. Visitors to the cryptocurrency site would then be redirected to the exploit kit landing page under certain conditions.

Maze ransomware makes use of RSA and ChaCha20 encryption technology as a part of the process, and it scans for documents to encrypt and appends different extensions to those files. The attacker of Maze ransomware takes different ransom amounts depending on the victim type such as a home computer, server or workstation, etc.

The threat has not been an idle one as the files of several companies have been released on the internet. The Maze ransomware is hard programmed with some tricks to prevent reversing of it and to make static analysis more difficult.

Impact of such Attack.

Maze ransomware was first discovered on 29 May 2019 therefore, this is a new type of ransomware which do not have much of a previous footprint. The attack of Maze has caused and will continue to cause an interruption to the different companies or businesses. This caused a loss of revenue and incremental costs that negatively impact the financial results. Despite being around for less than a year, Maze ransomware has wreaked havoc on businesses, municipalities all over the world, and been the subject of lawsuits, email impersonation attempts.

Cognizant publicly admitted April 18 that its network was infected with Maze ransomware, which ended up encrypting servers and taking out some of the company's work from home capabilities. Recovery and Mitigation Costs estimated worth $50 Million To $70 Million.

From 29 May 2019 to April 17, 2020, multiple attacks have been made by this ransomware. The impact of these attacks is known in some cases and others are unknown due to privacy laws and to protect the image of companies.

I am putting a list of attacks with the required information summary.

1. Attack on the Italian Revenue Agency was detected on 29 Oct 2019. Attack happened by a set of emails that came with a Word attachment that was using macros to run the ransomware in the system. This has been found by the Proofpoint of Italian agency.

These emails had targeted mainly manufacturing companies. Email enforces that the recipient should open and read the attachment to avoid further tax assessment and penalties. The malicious document purported to be an RSA SecurID key used by the Italian Ministry of Taxation that must be enabled.

Once the content is enabled, malicious macro runs a PowerShell script, which downloaded and installed a Maze ransomware payload onto the victim's system. This allows the attacker to get backdoor access.

2. Another attack on Allied Universal's computers. This attack demanded approximately US$2.3 million to decrypt the entire network. Before encrypting any computer, the Maze actors claimed to always steal a victim's files so that they can be used to further leverage the victim to pay the ransom.

3. Maze ransomware encrypted data from the City of Pensacola, Florida, and demanded a US$1 million ransom for a decryption. The city mentioned on 11 December 2019 that it was slowly recovering with their mail servers back up and gradually most of their landlines restored. City employees were unable to access their computers or the internet until all the issues were resolved, according to a Pensacola.

4. Wire and cable maker Southwire was hit by Maze ransomware on 9 December 2019, which affected computing on a companywide basis. The Maze actors demanded approximately US$6 million of ransom paid it bitcoin.

How is Maze resolved?

Cognizant deployed its internal protection to contain the incident along with leading cyber defense firms.

As part of its activities, Cognizant remotely manages its customers by end-point clients, or agents, that are installed on customer's workstations to push out patches, software updates, and perform remote support services.

Cognizant started emailing their clients, stating that they had been compromised and included a "preliminary list of indicators of compromise identified through our investigation." Clients could then use this information to monitor their systems and further secure them.

The list of indicators IOCs included IP addresses of servers and file hashes for the kepstl32.dll, memes.tmp, and maze.dll files. These IP addresses and files are known to be used in previous attacks by the Maze ransomware actors.

How to protect yourself from Cyber-attacks?

Basic Rules:

- Don’t open email attachments or click on hyperlinks from unknown senders.
- Use your spam blocking or filtering tools to block unsolicited emails, instant messages, and pop-ups.
- Use passwords that are hard to guess and change them regularly. Do not store usernames and passwords on websites.
- Exercise caution when downloading files from the Internet. Only download from trusted sources.

Protect Your Computer

- Back up files on your personal computers regularly using an external hard drive.
- Don’t keep sensitive or private information stored on your computer. If you get hacked, information can be found.
- Don’t share access to your computer with strangers and turn off file-sharing.
- Use multi-factor authentication (MFA)
- Use complex passwords, managed through a password manager
- Limit access rights; give user accounts and administrators only the access rights they need and nothing more
- Make regular backups and keep them offsite and offline where attackers can’t find
- Patch early and patch often. Ransomware like WannaCry and NotPetya relied on unpatched vulnerabilities to spread around the globe
- Lockdown your RDP. Turn off RDP if you don’t need it

Conclusion

Ransomware keeps evolving, getting faster, smarter – and costlier – at every turn. With a full-scale ransomware attack costing on average an eye-watering USD 755,991. Therefore, it is essential to know what you're up against – and how to stay protected. Many ransomware attacks start with a malicious email. Attackers know it only takes one individual to let down their guide for them to get into your organization. Education to every employee and proper protection to every endpoint the key to protect yourself.

ISS World Ransomware attack

Abstraction.

ISS world is a Denmark-based facilities management firm with a market position at 65+ workplaces around the world. On Feb 17, 2020 ransomware attack happened which is treated as the biggest attack of 2020 of recovery and mitigation cost around $75 Million To $112.4 Million respectively.

Introduction.

On Feb. 17 ransomware attack forced Denmark-based facility management firm ISS World. ISS is the world's one of the biggest companies in terms of the number of staff. They provide building services and other facilities like management to many banks, insurers, and other large enterprises.

When they revealed this attack, one good thing they did is to switch off their networks. Although this impacted their hundreds of thousands of employees without access to their systems or email.

Three days later, ISS World said that the root cause of the attack was weak cyber defense of their IT infrastructure. It had been identified and the company was working with outside experts to gradually restore their IT systems. They could not be able to disclose that whether this attack was falling in the category of Sodinokibi, or ReVIL, attacks.

ISS world has an inferior cybersecurity posture in several dimensions, compared to its peers.

- Network security – Encryption certificates revoked. MySQL database was visible.
- DNS health – Systems can be exploited, to run spoofing and denial of service attacks on others.
- Patching- unpatched software and even some end of service software still running.
- Application security- visitors to some ISS websites were vulnerable to man-in-the-middle attacks.

Impact of Attack.

As per the report from various channels, the attack happened on 17 February. ISS has taken precautionary measures and as their standard operating procedure, they immediately disabled access to shared IT services across their sites and countries,

which ensured the isolation of the incident.

Further, the root cause has been identified as a ransomware attack due to poor security posture and the company worked with forensic experts, their hosting provider, and a special external taskforce to gradually restore their IT systems.

Impact of attack happened in several ways right from the day attack discovered and recovery cost of their system and impact on their employees has been analyzed and estimated - around $75 Million To $112.4 Million. ISS estimated that it expects to restore and rebuilding of its systems and IT assets by the end of 2020.

This attack cause company to switch off its networks and disappeared from the web leaving hundreds of thousands of employees – including 43,000 in the UK – without access to their systems or email.

As a precautionary measure and as part of our standard operating procedure, the company immediately disabled access to shared IT services across their sites and countries, that helped to ensure the isolation of the incident.

How is this resolved?

ISS worked multifold to resolve the problem and took several measures as follows –

1. As a precautionary measure and as part of their standard operating procedure, they immediately disabled access to shared IT services across their sites and countries, which ensured the isolation of the incident. ISS was able to restore some systems early into the attack and said it initially did not see any evidence of the compromise of customer data. Still, the attack left the 43,000 employees of the company without access to email or other online services, according to reports. Its shares traded down around 3.5% shortly after the announcement and further dropped by 23% by Feb 26.

2. Later they identified the root cause and worked with forensic teams, hosting providers, and a special task force to gradually restore their IT systems.

3. They checked with their client and confirmed that no client got impacted because of this attack. The reason because its global network of employees generally works not in offices but at client facilities to ensure day-to-day operations run efficiently.

4. They are still expecting to spend $45 million to $75 million for remediating the IT incident; establishing workarounds to enable the continuous delivery of service and service underperformance due to system down-time; and cost duplication associated with contract operation. A rebuild of part of ISS's IT infrastructure due to damage to some of the company's IT assets is expected to cost between $22.5 million and $45 million.

How to protect yourself from Cyber attacks?

Some of the aspects are important in general for any malware attack including ransomware attack.

Use strong passwords - and don't re-use passwords, ever again.

Practice regular backups – This will help a lot as your last line of defense against a hug ransom demand. Be sure to keep them offsite where attackers can't find them.

Patch early, patch often- Many attacks example- WannaCry and NotPetya relied on unpatched vulnerabilities to spread themselves around the globe.

Lockdown RDP - Criminal gangs exploit weak RDP credentials to launch targeted malware attacks. Turn off RDP if you don't need it, and use rate-limiting, 2FA or a VPN if you do.

Apply anti-ransomware protection – Software such as Sophos Intercept X and XG Firewall are designed to work to combat ransomware and its effects. Individuals can protect themselves with Sophos Home.

Conclusion

The primary reason these incidents have become more disruptive and thus more financially damaging, according to a report is because they are increasingly moving beyond IT assets and disrupting operational technology (OT), which is traditionally separate from IT but increasingly merged due to digital transformation efforts. This is what enables cyber criminals to directly impact production processes.
The rising threat of business disruptions places an increasing premium demand on strong cyber governance and the need to better balance security with growth and cost targets.