Grant Thornton

An instinct for growth™

Cyber

Data

Security

Cyber attack: Maze ransomware

April 2020

Maze ransomware: A global security challenge

In recent times, large companies have grappled with ransomware threats from various cyber black hat hacker groups, who have become even more active following the Coronavirus pandemic, resulting in data breach and loss of reputation. A Maze ransomware attack can spread through a network, extract data from compromised systems and lock the users or encrypt data. With control over one's system and data, the ransomware actors ask for ransom or threaten to publish extracted confidential data on darknet for sale.

Below are some recent incidents

- One of the leading UK-based medical research company's computer systems were hacked by a Maze ransomware group.[1] As company denied to pay the ransom, this group uploaded the personal details of its patients on darknet for sale.
- A leading IT company identified the traces of Maze ransomware attacks on its network.[2] As part of their initial assessment, they came across preliminary list of indicators of compromise (IOCs) containing the IP addresses and file hashes that have been used by Maze ransomware actors in similar attacks in the past.

Cyber attack

Here's how a typical Maze attack works:

- Maze ransomware is often delivered via emails or exploit kits such as 'Fallout' and 'Spelevo'.
- '2048-bit RSA' and 'ChaCha20' stream of ciphers are used for encrypting files on the victim's machine.
- Random file extensions used by Maze include .ini, .gtfh, .ILnnD, among others.
- Further to encryption, it displays a message about the encrypted files and the file name of the dropped ransomware note.
- A notable feature of Maze ransomware is that it sets the ransomware amount based on the type of system it detects, such as standalone server, backup server, home computer/ workstation, etc.

1) https://www.databreaches.net/uk-medical-firm-poised-for-work-on-coronavirus-had-been-hit-by-maze-ransomware/
2) https://economictimes.indiatimes.com/tech/internet/cognizant-hit-by-maze-ransomware-attack/articleshow/75228505.cms?from=mdr

Maze ransomware attacks in the news

Targeting an Italian revenue agency, the actors instructed users to open an attached Microsoft Word document, claiming that it contained guidelines provided by the revenue agency.[3]

A Switzerland-based cybersecurity insurance provider that helps businesses deal with data breach is currently investigating a "security incident" that has made it a victim of data breach itself.[4]

The attack on an independently-owned supermarket chain based in Michigan and a leading insurance firm based out of Canada has resulted in lockdown of their internal systems.[5]

In 2019, sensitive data was stolen from an American security staffing company and a ransom worth 300 bitcoins (est. USD 2.3 million then) was demanded to decrypt the data.[6]

3) https://www.bleepingcomputer.com/news/security/maze-ransomware-attacks-italy-in-new-email-campaign/
4) https://www.techradar.com/in/news/maze-ransomware-hits-insurance-giant-chubb
5) https://searchsecurity.techtarget.com/news/252475822/Two-attacks-on-Maze-ransomware-list-confirmed
6) https://www.techrepublic.com/article/how-ransomware-attackers-are-doubling-their-extortion-tactics/

Challenges during COVID-19 that may increase the risk of Maze ransomware attacks

- In the current COVID-19 situation, a large section of the workforce is working from home using company devices or, in some cases, personal devices. These devices may not be receiving regular security updates.
- Risk of employees downloading and using unauthorised softwares.
- Risk of employees clicking on malicious links and opening phishing emails.
- Use of insecure remote connection to access clients' networks.
- No segregation of critical systems in the network.
- Not having up-to-date backup of critical data.
- Use of weak credentials.
- Improper logging and monitoring.
- Lack of antivirus definition updates.

Cyber security checklist

- ☑ Run periodic file backups. This backup files should be isolated from the network.
- ☑ Ensure antivirus definition is updated frequently.
- ☑ Latest security patches should be applied on all end points.
- ☑ Remote desktop connections that are not needed should be avoided.
- ☑ Avoid opening suspicious emails and attachments. Do not click on unknown links in emails.
- ☑ Disable macros in Office programs.
- ☑ Install ad blockers to combat exploit kits (for example: Fallout) which are distributed via malicious advertising.
- ☑ Since zero-day attacks are difficult to identify, it is always good to follow best security practices and perform proactive security test to determine security loopholes.
- ☑ Carry out threat hunting and red teaming exercises to prevent such attacks.
- ☑ Update browsers and plugins with the latest security patch as Spelevo exploits outdated browser plugins.
- ☑ Monitor logs and events for anomalies.
- ☑ Implement 'YARA' rule to detect Maze ransomware dll.
- ☑ Blacklist malicious IPs, URLs and other IOCs related to the maze ransomware.

Here's how our experts can help

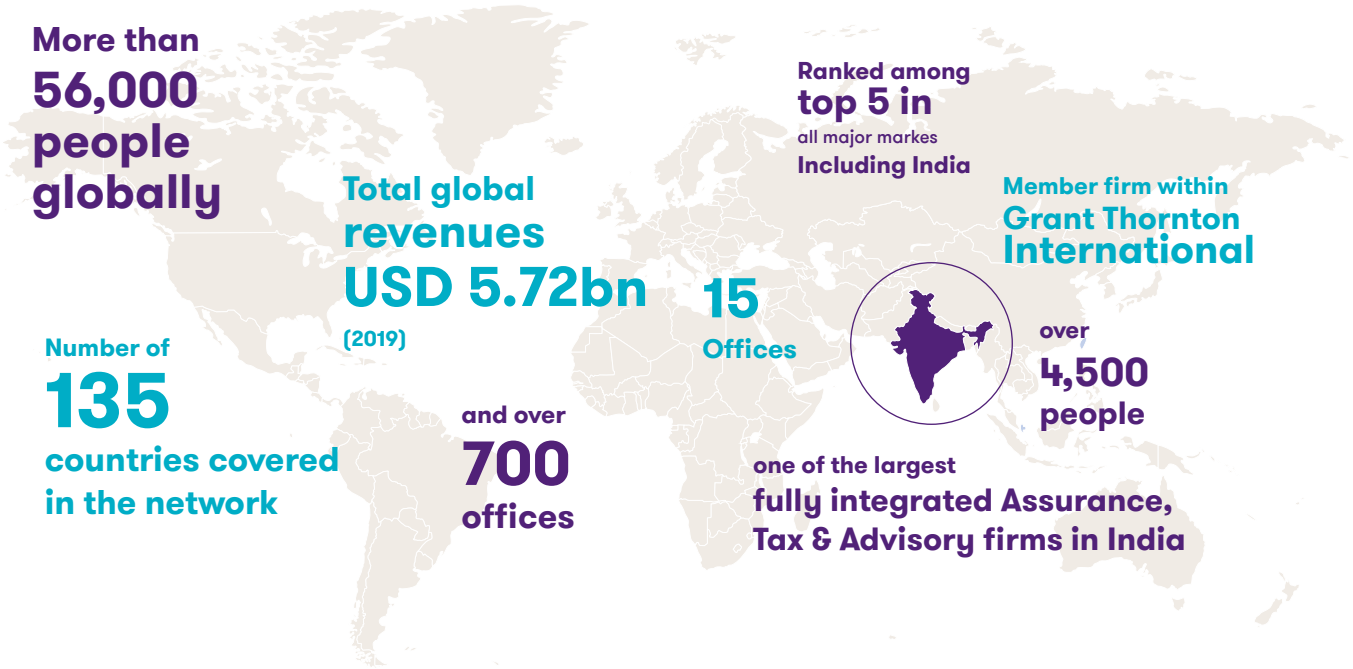
Grant Thornton in India has a team of experienced professionals who have assisted leading companies across verticals including financial services, technology, consumer and industry in conducting cyber security assessments and building cyber security frameworks deal with sophisticated cyber attacks. We also provide remediation assistance and help our clients in prevention of such attacks.

To know more abour our solutions, please contact:

Dinesh Anand
National Managing Partner, Risk
E: dinesh.anand@in.gt.com

Akshay Garkel
Partner, Cyber
E: akshay.garkel@in.gt.com

About Grant Thornton in India



Contact us

To know more, please visit www.grantthornton.in or contact any of our offices as mentioned below:

NEW DELHI
National Office
Outer Circle
L 41 Connaught Circus
New Delhi 110001
T +91 11 4278 7070

NEW DELHI
6th floor
Worldmark 2
Aerocity
New Delhi 110037
T +91 11 4952 7400

AHMEDABAD
7th Floor,
Heritage Chambers,
Nr. Azad Society,
Nehru Nagar,
Ahmedabad - 380015

BENGALURU
5th Floor, 65/2, Block A,
Bagmane Tridib, Bagmane
Tech Park, C V Raman Nagar,
Bengaluru - 560093
T +91 80 4243 0700

CHANDIGARH
B-406A, 4th Floor
L&T Elante Office Building
Industrial Area Phase I
Chandigarh 160002
T +91 172 4338 000

CHENNAI
7th Floor,
Prestige Polygon
471, Anna Salai, Teynampet
Chennai - 600 018
T +91 44 4294 0000

DEHRADUN
Suite no. 2211, 2nd floor Building
2000, Michigan Avenue,
Doon Express Business Park
Subhash Nagar, Dehradun - 248002
T +91 135 2646 500

GURGAON
21st Floor, DLF Square
Jacaranda Marg
DLF Phase II
Gurgaon 122002
T +91 124 462 8000

HYDERABAD
7th Floor, Block III
White House
Kundan Bagh, Begumpet
Hyderabad 500016
T +91 40 6630 8200

KOCHI
6th Floor, Modayil Centre point
Warriam road junction
M. G. Road
Kochi 682016
T +91 484 406 4541

KOLKATA
10C Hungerford Street
5th Floor
Kolkata 700017
T +91 33 4050 8000

MUMBAI
16th Floor, Tower II
Indiabulls Finance Centre
SB Marg, Prabhadevi (W)
Mumbai 400013
T +91 22 6626 2600

MUMBAI
Kaledonia, 1st Floor,
C Wing (Opposite J&J office)
Sahar Road, Andheri East,
Mumbai - 400 069

NOIDA
Plot No. 19A,
7th Floor
Sector – 16A
Noida 201301
T +91 120 485 5900

PUNE
3rd Floor, Unit No 309 to 312
West Wing, Nyati Unitree
Nagar Road, Yerwada
Pune- 411006
T +91 20 6744 8800

For more information or for any queries, write to us at ITRiskAdvisory@in.gt.com

Follow us @GrantThorntonIN