MAZE RANSOMWARE BREACHED IT SUPPORT GIANT "COGNIZANT"

OVERVIEW

**Breach Alert:** Maze Ransomware Breached IT Support Giant “Cognizant”  
**Published:** 2020-04-20  
**Threat Level:** High  
**Status:** Initial

In the worldwide outbreak of COVID-19, Opportunistic cybercriminals are leveraging it to conduct[1] mass cyber-attacks across Indian Cyberspace targeting different sectors.

On April 17, 2020, according to the highly credible source, it was revealed that the US IT giant Cognizant was experiencing a possible ransomware attack that led to customer notifications. The attribution behind the attack is suspected to be Maze with high confidence.

A threat actor, named “TA2101” by ProofPoint, has been using a variant of the ChaCha ransomware, known as Maze ransomware. So, it is highly suspicious that these threat actors are behind this incident as well.

MAZE is a ransomware that has the functionality to spread remote and removable drives and employs several anti-debugging and anti-disassembly techniques. It escapes encryption routine on some files, extensions and directory names based on a pre-defined list. The payment instruction is written in an image (bitmap) file in the Temp folder, and a text file (e.g. DECRYPT-FILES.txt) placed in each directory where files are encrypted. It also collects and sends system information to hard-coded IP addresses via HTTP POST using randomly selected URI strings and HTML extensions.

Maze ransomware is commonly spread using email spams and Exploit kits like Fallout and Spelevo.

Once it infects a machine, it not only encrypts the files but also exfiltrates data allowing the malicious actor to use it as an opportunity for additional leverage or ransom. The Maze has the ability even to infect mission-critical systems; this might lead to considerable ransom demands on the disruption of maximum services[2].

The malicious artefacts could be masked under the guise of controlled botnet attacks or spear phishing attachment campaigns. Some threat actors are disguising their malicious emails under the pretence of providing information to the user on how to protect themselves from the virus, updates regarding the virus and ask the victims to click on links, pdf, mp3 or docx files associated to the same[1].
CRITICAL ADVISORY

These files or network artefacts are capable of hosting a range of threats from Trojans to worms. Not only are they intelligent enough to interfere with the operation of computers/ computer networks but also are capable of destroying, modifying, blocking or copying data when users visit the website or click on any hyperlink redirected to the malicious website[1].

Hence, we as CPF team along with our volunteers & security researchers, have planned to work on identification, investigation to reporting such cases of potential malware outbreaks or Ransomware to proactively safeguard CII & corporate houses, industries from being the victim of any such attacks.

TASK & OBJECTIVE

We have run multiple OSINT crawler and identified several indicators like IP, domain, malware hash etc. & other subjective information to identify threat actor, their behaviour and controls required to detect and prevent such attack.

BEHAVIOUR PROFILING

1. Once the malware executes, the following two conditions are checked to determine whether a system needs to be infected or not.

Checks for specific file present in the system.

For MD5: BD9838D84FD77205011E8B0C2BD711E0, following file path is checked: "C:\\JDUIHluf\\IDisjopjcnb". If the file is present, then the malware terminates without infecting. (Fig-1)

Checks for the command-line parameter of the process.

For MD5: BD9838D84FD77205011E8B0C2BD711E0, following command-line parameter is checked: "--Dldsjdjdj". If command-line matches, the ransomware terminates without infection. (Fig-2)[2]
2. Once the above two conditions are validated, the malware launches a routine that locates and decrypts the MAZE-Ransomware payload. This is stored inside RC_DATA of restores structure. It is further also disguised as a png file so that the RC_DATA stores a png file but once the png file structure ends, the encrypted payload is present.

3. The malware then allocates memory. It also changes the permission of the memory to "PAGE_EXECUTE_READWRITE" further even decrypting the encrypted data on this memory.

4. To perform decryption of the encrypted code, three levels of decryption are performed on the data.
   
   i. XOR decryption
   The XOR decrypted data is encoded with Base64 algorithm.
   
   ii. Base64 decode
   The malware performs Base64 decoding by loading Crypt32.dll and calling CryptStringToBinary to decode the encoded data.
   
   iii. The decoded data is again decrypted to get the final shellcode and Maze Ransomware executable.

5. Once decrypted, the Maze ransomware is loaded into memory and creates a thread to the Maze ransomware

6. The Ransomware also terminates the monitoring tool (Procmon.exe) if it is found running in the system.

7. Once the ransomware code starts executing, it searches for shadow copy and deletes the shadow copy from the system. To delete the shadow copy, it uses the wmic.exe tool.

8. The Ransomware begins enumerating the directories and files to encrypt. After this encryption process ends, a ransomware note is dropped along with instructions on payment of the ransom to attain the decrypting tool. Maze ransomware uses the ChaCha algorithm (Similar to Salsa20) and RSA-2048 algorithm to encrypt files.

9. All the encrypted files are renamed and appended with a random extension. Maze ransomware collects information related to each system, identifies the system is a server or connected to a node in a corporate network, and categorizes each order.

10. The dropped ransomware note contains the following information:
   
   a. Link to download TOR browser.
   b. Link to .onion site to contact ransomware operators.
   c. Identification key at the end of ransom-note[2]
CRITICAL ADVISORY

STAGES OF MAZE RANSOMWARE INFECTION

First Stage:

PE executable is dropped as random filename into a low-privilege folder, calling another function by using CreateTimerQueueTimer API to evade detection. The function is imported and abused to execute target_function, which contains a decryption code of trailing data. A total of 370 KB of shellcode are decrypted using the HC-128 algorithm, with fixed key and initialization vector.

Second Stage:

In the second stage, the large shellcode is executed. Shellcode imports functions used to do reflective DLL loading using a large chunk of data post shellcode to hide it from the process module list.

Third Stage:

In the third stage, the main functionality of the Ransomware relies on the hidden DLL loaded by the shellcode at the second stage. The code is highly obfuscated, with a few tricks to make reverse engineering harder. It employs multi-level obfuscation, evasion & privilege escalation techniques also to hide the flow of exploitable code.

We found that the first exploit targets the CVE-2016-7255 vulnerability in win32k.sys. The vulnerability was described in detail by TrendMicro[4], then a patch analysis was made by researchers at McAfee[5].

However, the second exploit is a more recent privilege escalation exploit targeting the CVE-2018-8453 vulnerability in win32k.sys. The vulnerability has been described by Kaspersky, patch analysis was made by 360A-TEAM in their article[6], and was also analyzed by QianXin TI Center in their write-up[7].

RANSOMWARE ACTIVITY:

1. Fingerprinting of Computer
2. Backup Deletion
3. File Scanning
4. File Encryption
5. Encryption keys
6. Key persistence
7. Network connections to C2 hosts
ATTACK CHAINS:

Target Receives Microsoft Word 2007+ Document

Macro Downloads Maze Ransomware

Maze Encrypts Files Using 2048 Bit RSA and ChaCha 20

Maze Sends HTTP POST Request to IP URLs

hXXp://91.228.144.7/*

Maze Drops Ransom Note

INSIGHTS:

1. Registrar Information

Source ASN: Russian Federation
AS: 49335
Country: RUSSIA
Registration Date: 2009-05-20
Registrar: ripencc
Owner: NCONNECT-AS, RU

ASSOCIATED EMAIL ADDRESSES: filedecryptor@nuke.africa

IOC USED ( HASH /// FILE VALUE )

1. e8a091a84dd2e7ee429135f48e9f48f7787637ccb79f6c3eb42f34588bc684 /// Ransom.Win32.MAZE.H
2. 9d86beb9d4b07dec9db6a692362ac3fcej2275065194a3bda739fe1df49f9c7 /// out
3. 5c9b7224ff2d029b6ce7b82ea40d63b9d4e4f502169bc91de88b4ea577f52353 /// 1-1.exe
4. 7e3ab96d2628e0a9970802b47d0356dc9b999944d7f98492d4e70a5384891695a /// USPS_Delivery.doc
5. d617fd4b2d0828a1a7eb9693c6ec6e71447d501d24653a8e99f9e12136491a8 /// R19340003422.doc
6. 9f2139cc7c3fad7f133c26015de3310981de26d7f1481355806f430f9c97e639 /// VERDI.DOC
7. cfd8e3a47036c4e6eb318117c0c23e1266ae95d1774da37d5b6c3de02bdfe2a /// VERDI.doc
8. 806fc33650b7ec35dd01a06be3037674ae3cc0db6ba1e3f690ee9ba9403c0627 /// wordupd.tmp, wudp12.14.tmp
9. 0F841C633289EA27CAC1C49D5B1D35B.mlw
10. d728b57f8f70fa1fe24c616c59f72242bf52bc85de1d8e1d86623b0556b1c /// LOAD__ENCDLL.EXE
11. cdcce1615f46852e81dd770c55869b9bc92befff38d82024878f2e0520b5a2d /// winupd.tmp, win163.65.tmp, jdrk.exe, JDRK.EXE
CRITICAL ADVISORY

IP:
1. 5.199.167.188
2. 45.76.149.204
3. 91.218.114.4
4. 91.218.114.11
5. 91.218.114.25
6. 91.218.114.26
7. 91.218.114.31
8. 91.218.114.32
9. 91.218.114.37
10. 91.218.114.38
11. 91.218.114.77
12. 91.218.114.79
13. 92.63.8.47
14. 92.63.11.151
15. 92.63.15.6
16. 92.63.15.8
17. 92.63.15.56
18. 92.63.17.245
19. 92.63.29.137
20. 92.63.32.2
21. *92.63.32.55
22. 92.63.37.100
23. 92.63.194.3
24. 92.63.194.20
25. 104.238.158.250
26. 104.168.174.32
27. 104.168.198.208
28. 104.168.198.230
29. 104.168.201.35
30. 104.168.201.47
31. 104.168.215.54
32. 146.0.72.85
33. 149.56.245.196
34. 185.147.15.22
35. 195.123.217.13
36. 198.50.168.67
37. 192.99.172.143

DOMAINS:
1. introle[.]biz
2. aoacugmutagkwctu.onion
3. plex[.]direct
4. agenziaentrates[.]icu
5. agenziaentrateinformazioni[.]icu
6. agenzialinformazioni[.]icu
7. bzst-info[.]icu
8. hilfe-center-1und1[.]icu
9. intralian[.]icu
10. usps-deliveryservice[.]icu
11. zhengjuncal[.]monster
12. healtyproductbest[.]review
13. download-invoice[.]site
14. malaysiaterkini[.]site
15. conbase[.]top
16. mazedecrypt[.]top
17. condurises[.]xyz
18. emplementriaton[.]xyz
19. fantlimit[.]xyz
20. heatmoscver[.]xyz
21. publistendick[.]xyz
22. thistrich[.]xyz
23. suceptishough[.]xyz
24. throposion[.]xyz
25. werenceptical[.]xyz
26. yearinesents[.]xyz
27. 1drivelive[.]com
28. aloha-edc[.]net
29. gsitestat[.]com
30. nesinoder[.]com
31. set-validator[.]com
32. wwwcoinbase[.]com
33. canadian-overnite[.]com
34. info-delivery-notification[.]com
35. lj-kabel[.]net
36. hotspot.easygonet[.]com
37. webislem[.]kibrisonline[.]com
38. activate[.]netonline[.]net
<table>
<thead>
<tr>
<th>Number</th>
<th>Domain</th>
<th>Number</th>
<th>Domain</th>
</tr>
</thead>
<tbody>
<tr>
<td>39</td>
<td>bayi.netonlined.net</td>
<td>77</td>
<td>dependepeal[].info</td>
</tr>
<tr>
<td>40</td>
<td>beta-bayi[].kibrisonline[].com</td>
<td>78</td>
<td>mostualled[].info</td>
</tr>
<tr>
<td>41</td>
<td>dev-bayi[].netonlined.net</td>
<td>79</td>
<td>all-apk[].info</td>
</tr>
<tr>
<td>42</td>
<td>dev-hotspotpanel[].netonlined.net</td>
<td>80</td>
<td>apkbit[].info</td>
</tr>
<tr>
<td>43</td>
<td>gidra2web[].shop</td>
<td>81</td>
<td>apkesey[].info</td>
</tr>
<tr>
<td>44</td>
<td>gidraruxzpnew4aff[].com</td>
<td>82</td>
<td>apkfinder[].info</td>
</tr>
<tr>
<td>45</td>
<td>gudra2wed[].com</td>
<td>83</td>
<td>apk-get-update[].info</td>
</tr>
<tr>
<td>46</td>
<td>gudra2wep[].com</td>
<td>84</td>
<td>apkhia[].info</td>
</tr>
<tr>
<td>47</td>
<td>gybra2web[].com</td>
<td>85</td>
<td>apkitsall[].info</td>
</tr>
<tr>
<td>48</td>
<td>gydra2web[].co</td>
<td>86</td>
<td>apks-rec[].info</td>
</tr>
<tr>
<td>49</td>
<td>gydra2web[].shop</td>
<td>87</td>
<td>apk-rool[].info</td>
</tr>
<tr>
<td>50</td>
<td>gydra2wed[].com</td>
<td>88</td>
<td>apkrool[].info</td>
</tr>
<tr>
<td>51</td>
<td>gydra2wep[].com</td>
<td>89</td>
<td>apk-tools[].info</td>
</tr>
<tr>
<td>52</td>
<td>hedra2web[].com</td>
<td>90</td>
<td>apktool[].info</td>
</tr>
<tr>
<td>53</td>
<td>hibra2web[].com</td>
<td>91</td>
<td>apktwin[].info</td>
</tr>
<tr>
<td>54</td>
<td>hidra2wed[].com</td>
<td>92</td>
<td>apk-update[].info</td>
</tr>
<tr>
<td>55</td>
<td>hidra2wep[].com</td>
<td>93</td>
<td>appsfans[].info</td>
</tr>
<tr>
<td>56</td>
<td>hudra2wed[].com</td>
<td>94</td>
<td>bit-apk[].info</td>
</tr>
<tr>
<td>57</td>
<td>hudra2wep[].com</td>
<td>95</td>
<td>freshapk[].info</td>
</tr>
<tr>
<td>58</td>
<td>hybra2web[].co</td>
<td>96</td>
<td>get-apk-update[].info</td>
</tr>
<tr>
<td>59</td>
<td>hydra2web[].com</td>
<td>97</td>
<td>instaapk[].info</td>
</tr>
<tr>
<td>60</td>
<td>hydr2aweb[].com</td>
<td>98</td>
<td>pure-apk[].info</td>
</tr>
<tr>
<td>61</td>
<td>hydra2wewb[].com</td>
<td>99</td>
<td>qwecklyapk[].info</td>
</tr>
<tr>
<td>62</td>
<td>hydra2ved[].com</td>
<td>100</td>
<td>to-apk[].info</td>
</tr>
<tr>
<td>63</td>
<td>hydra2wed[].co</td>
<td>101</td>
<td>true-apk[].info</td>
</tr>
<tr>
<td>64</td>
<td>hydra2weg[].com</td>
<td>102</td>
<td>trueapk[].info</td>
</tr>
<tr>
<td>65</td>
<td>hydra2wep[].co</td>
<td>103</td>
<td>upd-ur-apk[].info</td>
</tr>
<tr>
<td>66</td>
<td>hydra4web[].com</td>
<td>104</td>
<td>update-ur-apk[].info</td>
</tr>
<tr>
<td>67</td>
<td>hydrowed[].com</td>
<td>105</td>
<td>sicurezza[].me</td>
</tr>
<tr>
<td>68</td>
<td>hydrow2ep[].com</td>
<td>106</td>
<td>mx2[].mgk[].pl</td>
</tr>
<tr>
<td>69</td>
<td>onion[].business</td>
<td>107</td>
<td>fermer[].ru</td>
</tr>
<tr>
<td>70</td>
<td>onion[].capital</td>
<td>108</td>
<td>itfermer[].ru</td>
</tr>
<tr>
<td>71</td>
<td>onion[].cards</td>
<td>109</td>
<td>libin[].ru</td>
</tr>
<tr>
<td>72</td>
<td>onion[].fish</td>
<td>110</td>
<td>bayi[].netcity[].net[].tr</td>
</tr>
<tr>
<td>73</td>
<td>onion[].limited</td>
<td>111</td>
<td>shop[].nethouse[].net[].tr</td>
</tr>
<tr>
<td>74</td>
<td>onion[].management</td>
<td>112</td>
<td>missiondirectorates[].us</td>
</tr>
<tr>
<td>75</td>
<td>onion[].photo</td>
<td>113</td>
<td>sresponsiblesd[].us</td>
</tr>
<tr>
<td>76</td>
<td>onion[].shopping</td>
<td>114</td>
<td>nano-care[].vn</td>
</tr>
</tbody>
</table>
MALICIOUS NETWORK CONNECTION

1. hxxp://92.63.8.47
2. hxxp://92.63.32.2
3. hxxp://92.63.37.100
4. hxxp://92.63.194.20
5. hxxp://92.63.17.245
6. hxxp://92.63.32.55
7. hxxp://92.63.11.151
8. hxxp://92.63.194.3
9. hxxp://92.63.15.8
10. hxxp://92.63.29.137
11. hxxp://92.63.32.57
12. hxxp://92.63.15.56
13. hxxp://92.63.32.52
14. hxxp://92.63.15.6

Maze ransomware doesn’t just demand payment for a decryptor but exfiltrates victim data and threatens to leak it publicly if the target doesn’t pay up.

This "double whammy" piles on yet more pressure to convince the victim to cave into the cybercriminals’ demand.

Note: If organizations detect any of the hashes above on their systems, the filenames associated with the hashes may be different than those identified in the right hand

MITIGATIONS:

Generic Recommendations

It is highly likely that given the concerning situation, there will be more of such threat actors who will conduct such malicious activities taking advantage of the global situation. Users are reminded not to click on Links/URLs or open attachments found in suspicious-looking emails or messages[1].

Technical Recommendations

To protect systems from Maze ransomware, Cyber Peace Foundation recommends organizations ensure:

1. Personnel know how to identify phishing emails, and update the phishing database and put identified domains onto block mode from internal systems.
2. Endpoint protection suite is applied and updated daily.
3. McAfee Virus Scan Enterprise – KB81095 & KB54812.
4. McAfee EPO – KB86007
5. Windows - To disable the Autorun feature on Windows remotely using Windows Group Policies, refer to this article from Microsoft.

Ref: http://support.microsoft.com/kb/967715
Additional User Recommendations

1. Do NOT open Microsoft Office documents (docx, .doc) file attachments unless specifically requested by the sender.

2. View the email header or send a separate email to validate the sender before you open attachments.

3. A Macro is a type of feature that allows instructions to run in Microsoft Office programs. They are only active if the setting "Enable all macros" is toggled on, or a user manually toggles a macro on (by default they are off). It is recommended to Disable macros in Microsoft Office applications.

4. The recommended setting is the "Disable all macros with notification" option under "Macro Settings" setting.

5. In case a user device gets attacked by Ransomware, it may lose all data. Back up your business data to the organization's shared folders.

6. Suspicious emails should be reported to the organization's Security Operations Center and all co-workers and employees informed on where and how to submit suspicious emails.[2]

Yara Rules to detect Maze ransomware Payload

```
rule crime_win32_ransom_maze_dll_1
{ meta:
  description = "Detects Maze ransomware payload dll unpacked"
  tip = "white" date = "2020-04-18"
  strings: $str1 = "Maze Ransomware" wide
  $str2 = "--logging" wide
  $str3 = "DECRYPT-FILES.txt" wide
  $stick_server_call = { ff ?? ?? 8b ?? ?? ?? ?? ?? ?? ff dd 8b ?? 89 f9 50 ff ?? ?? ff d6 8d ?? ?? ?? 89 ?? ?? ?? 56 e8 ?? ?? ?? ?? 83 c4 04 b9 66 66 66 69 89 c5 ff e9 89 d0 d1 fa c1 e8 1f 01 c2 8d ?? ?? 9c 56 e8 ?? ?? ?? ?? 83 c4 04 b9 56 55 55 89 c6 ff e9 89 f9 89 d0 c1 e8 1f 01 d0 8d ?? ?? ?? 29 c6 8b ?? 55 56 ff ?? ?? ?? 85 c0 0f ?? ?? ?? ?? 89 ?? ?? ?? 8b ?? ?? ?? ?? 89 c5 50 ff d3 89 c6 ff ?? ?? ?? ff d3 8b ?? ?? ?? 01 f0 3d ff 03 00 00 0f ?? ?? ?? ?? 55 ff ?? ?? ?? 68 a2 95 c3 00 53 ff ?? ?? ?? ?? ?? 83 c4 10 c6 ?? ?? c6 ?? ?? ?? ?? }
condition:
( uint16(0) == 0x5a4d and ( 3 of them ) or ( all of them ) )
```

Restart Mechanism: Once the machine was encrypted, there were no signs of any restart mechanism for MAZE Ransomware[2].
REFERENCES:

cious-cyber-activities-leveraging-wuhan-coronavirus-situation
content/live/CORP_KNOWLEDGEBASE/92000/KB92415/en_US/McAfee_Labs_Threat_Advisory_Maze.pdf
3. ( Threat Actor TA2101 [ProofPoint] using Maze Ransomware to ... https://www.fipco.com/solutions/it-au-
4. https://blog.trendmicro.com/trendlabs-security-intelligence/o-
one-bit-rule-system-analyzing-cve-2016-7255-exploit-wild/
5. https://www.mcafee.com/blogs/other-blogs/mcafee-labs/dig-
ging-windows-kernel-privilege-escalation-vulnerability-cve-2016-7255/
6. From patch diff to EXP, CVE-2018-8453 vulnerability analysis and exploitation, 360A-TEAM: https://mp.wei-
xin.qq.com/s/ogKCo-Jp8vc7otXyu6fTig
7. https://t1.360.net/blog/articles/cve-2018-8453-win32k-eleva-
tion-of-privilege-vulnerability-targeting-the-middle-east-en/
10. https://twitter.com/VK_Intel/status/1251388507219726338
11. https://twitter.com/underthebreach/status/125160359409664005
ware-cnc-sigma-ioc-detectionrule-soc-prime
13. https://www.virustotal.com/gui/url/0f60dc133f486178bd13ac1f266b02c0ca6771e6a066fb419dd0e17
ed40a475eb/details
ces-giant-cognizant-suffers-mazeransomware-cyber-attack/
15. https://download.bitdefender.com/resources/files/News/CaseStu-
dies/study/318/Bitdefender-TRR-Whitepaper-Maze-create4351-en-EN-GenericUse.pdf
17. https://securityintelligence.com/news/spelevo-ek-exp-
loits-flash-player-vulnerability-to-deliver-maze-ransomware/
18. https://twitter.com/jeromeseagara/status/1133767240686288896
19. Microsoft advisory CVE-2018-8453:
cve2018-8453-used-in-targeted-attacks/88151/