Research ransomware released in 2015 or 2016. Please specify its name and working mechanism.

Ans:

Marsjoke (Trojan Cryptor Polygot)

Presently ransomware are one of the most popular and dangerous malware. Ransomware encrypts file of a system and asks ransom from the victim in order to receive the key for decryption. Discovered in sept 26 2016, Marsjoke, also known as polygot, is a type of ransomware that primarily targeted state and local government agencies and educational institutions in the United States. This ransomware, once infected, left its victim with 96 hours to pay the ransom before completely deleting the victim’s files. This ransomware is classified as Trojan as it tricks the user into clicking the executable.

Working Mechanism:

Polygot is spread mainly through spam, where an email is sent, seemingly containing important documents, but leading to a link through which the malicious executable files are downloaded. Marsjoke first changes the victim’s wallpapers, and then allows first five files to be decrypted for free. Once installed Marsjoke connects to a command-and-control server where the ransom is handled and information about the victim PC is sent. The ransomware affects the following most windows operating systems (except windows 10).

Once executed the ransomware creates the following files:

- %UserProfile%\My Documents\[RANDOM CHARACTERS].bmp
- %UserProfile%\My Documents\[RANDOM CHARACTERS].exe
- %UserProfile%\My Documents\My Music\[RANDOM CHARACTERS].exe
- %UserProfile%\Start Menu\Programs\Startup\[RANDOM CHARACTERS].exe
- %UserProfile%\Start Menu\Programs\Startup\x.vbs
- %AllUsersProfile%\Documents\!!!ForDecrypt!!!.exe
- %AllUsersProfile%\Documents\!!!ForDecrypt!!!.exe
- %AllUsersProfile%\Documents\[RANDOM CHARACTERS].exe
- %AllUsersProfile%\Documents\My Music\[RANDOM CHARACTERS].exe
- %AllUsersProfile%\Documents\My Pictures\[RANDOM CHARACTERS].exe
- %AllUsersProfile%\Documents\My Videos\[RANDOM CHARACTERS].exe
- [ALL FIRST LEVEL DIRECTORIES]\!!! For Decrypt !!!.bat
- [ALL FIRST LEVEL DIRECTORIES]\!!! Readme For Decrypt !!!.txt

To change the windows configuration for its convenience (ex: running ransomware everytime the windows restarts) the following registries are affected:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\My Music\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\My Pictures\[RANDOM CHARACTERS].exe"

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\My Videos\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "%UserProfile%\My Documents\My Music\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\"[RANDOM CHARACTERS]" = "%UserProfile%\My Documents\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\My Music\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\My Pictures\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\My Videos\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\"[RANDOM CHARACTERS]" = "%AllUsersProfile%\Documents\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\"[RANDOM CHARACTERS]" = "%UserProfile%\My Documents\My Music\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\"[RANDOM CHARACTERS]" = "%UserProfile%\My Documents\[RANDOM CHARACTERS].exe"
- HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Windows\"Run" = "%UserProfile%\My Documents\[RANDOM CHARACTERS].exe"

The ransomware connects to the following links for command-and-control server:

- [http://]drec5tbop7q6uwvz.onion.link
- [http://]kr36yggvf2kpps2k.onion.link
- [http://]kauy4vb5tep6mhfc.onion.link
- [http://]buxnfuoim27a3yvh.onion.link
- [http://]rf2rnm5nbkxnkhua.onion.link

While executing the ransomware creates the mutex HelloWorldItsJokeFromMars so that resources are allocated properly among threads.

On User Interface part, Marsjoke has many similarities, from text look and request failed window, with CTB-Locker ransomware. Researcher believe that this similarity is intentional and is an attempt to fool the researchers, as they share no code similarities.

Recommendation:

Due to a mistake in the key generator, researcher from Kaspersky Labs have been able to find a cure. To decrypt the files encrypted by polygot RannohDecryptor utility (version 1.9.3.0 or newer) can be used. This software however does not work with the newer version of polygot, so the only solution here would be awareness amog users. Users should not readily open emails from unknown person and before installing any program the program must be scanned. Users with more technical experience can analyze the binary, and check if the executable makes the changes in registry as mentioned in the working mechanism section.