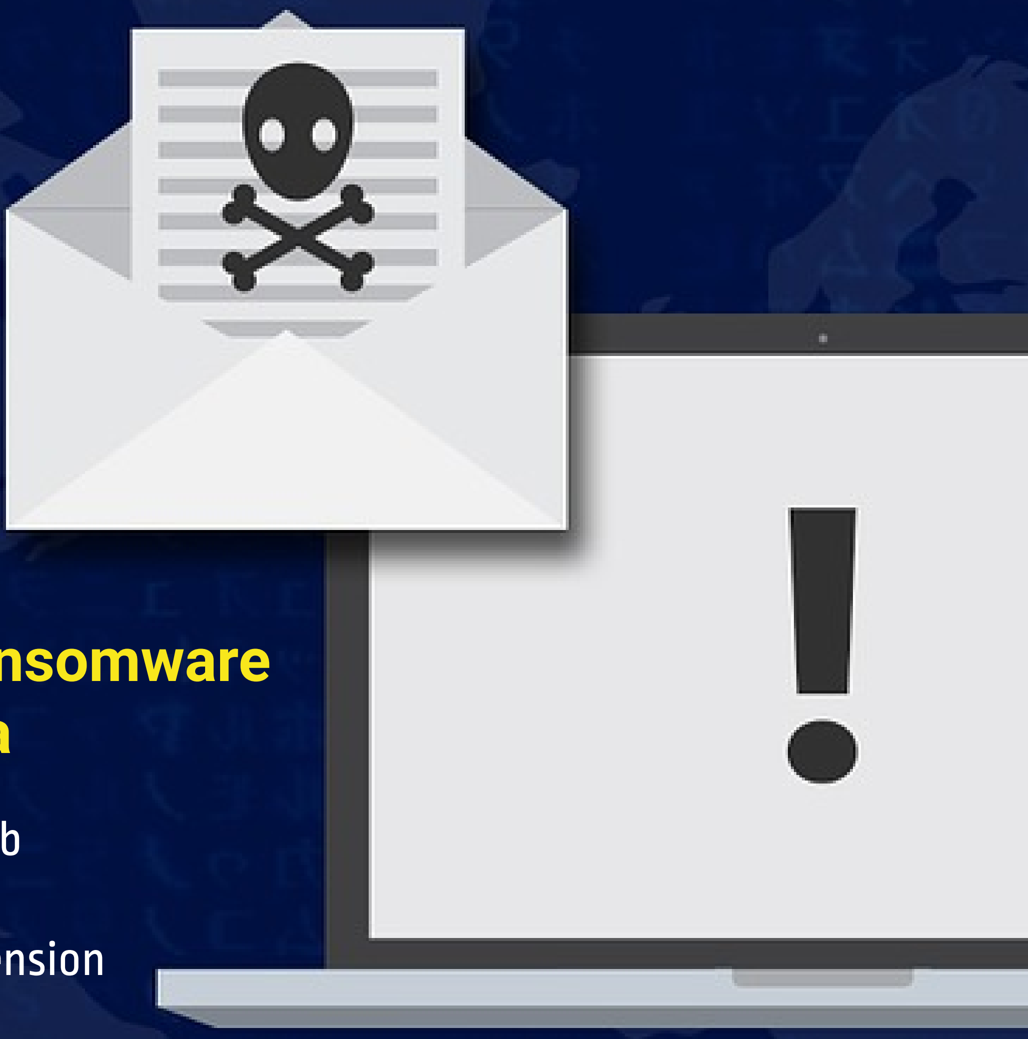
Everything About Jigsaw Ransomware

Jigsaw ransomware encrypts files on an infected system. After encryption, a ransom note is sent to user, asking for certain amount of bitcoins in order to get the files decrypted.

- Attackers blackmail victims to pay the ransom or they shall delete user files every hour.
- There are 226 different file types that are targeted by attackers including .jpg, .jpeg, .png, .docx, .xlsx and much more.
- The files are usually encrypted with an AES algorithm along with .FUN, .KKK, .GWS or .BTC extension in the file name.



How To Remove Ransomware & Restore Your Data

Find firefox.exe in startup tab present in the task manager window and disable the extension to stop it from launching at windows startup.

Disable the jigsaw ransomware process by opening the task manager (Ctrl + Shift + Esc) and terminate the firefox.exe and drpbx.exe processes.

In order to restore your system to previous date, go to the system protection tab present in system properties window and select 'system restore' option to begin the restoration process.

Tips To Prevent Jigsaw Ransomware

- Keep your system well protected by adding a antivirus tool in your system.
- Never open unusual email attachments since most ransomware's are initiated by attachments (email).
- Have a good backup system, just in case your system gets struck by Jigsaw ransomware & you are unable to retrieve the files.

www.thecentexitguy.com

Centex Technologies

CENTEX TECHNOLOGIES

13355 Noel Road,
Suite # 1100, Dallas, TX 75240
Phone: (972) 375 - 9654

501 N. 4th Street,
Killeen, TX - 76541
Phone: (254) 213 - 4740

1201 Peachtree St NE,
Suite 200, Atlanta, GA 30361
Phone: (404) 994 - 5074