

All About

CTB-Locker Ransomware

CTB-Locker i.e Curve-Tor-Bitcoin Locker is a variant of CryptoLocker & is extremely dangerous since it is hard to detect. This type of ransomware is often spread through emails that look legitimate.

How It Works

1. The attacker sends a spam email with an attached infected .zip file.

2. CTB-locker installs itself onto the victim's computer & then starts encrypting victim's files.



3. After infecting the computer, a message pops up on screen with the following message - 'Your personal files are encrypted'.

4. The attacker gives victim certain time to make the payment to get their data back. Failure to do so may lead to permanent loss of data.

Ways To Protect Yourself

Never click on suspicious emails or email with links or attachments sent from an unknown source.

Create backups of your data & store them separately.



Update your system software & applications regularly.

Stop or block all the binaries running from %TEMP% and %APPDATA% paths.

Opt for safe internet practices & never share confidential information in chat rooms or forums.

www.centextech.com
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