Dear All,

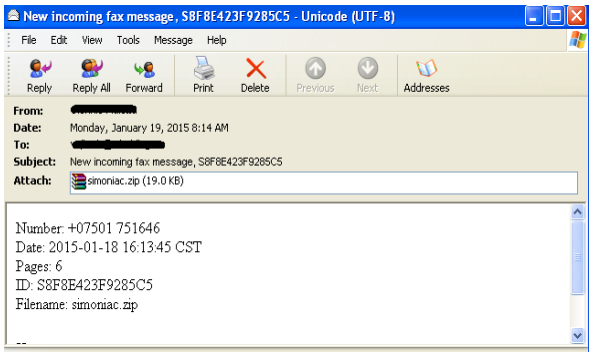
This is to bring to your notice that a new malware is being circulated through SPAM emails. Please treat the emails with the following subject lines under SPAM category and request you not to open such emails. Following is the description and symptoms of the malware for your reference:

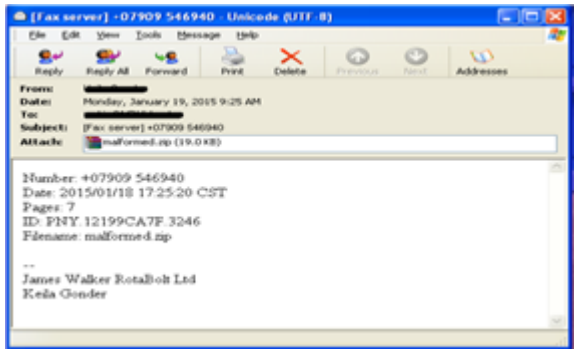
CTB-Locker is ransomware that on execution encrypts certain file types present in the user's system. The compromised user has to pay the attacker with a ransom to get the files decrypted.

Infection and Propagation Vectors

The malware is being propagated via spam emails; it comes with an attachment in the form of a .zip file. The .zip file is layered inside another .zip file, which contains the downloader for CTB-Locker.

The spam emails may appear similar to the following:





The attachments in the spam emails are .zip files, some of which may be named as one of the following:
malformed.zip plenitude.zip inquires.zip simoniac.zip faltboat.zip incurably.zip payloads.zip dessiatine.zip

The subjects used in the spam campaign may be named as one of the following:

[Fax server] +07909 546940 copy from +07540040842
Message H4H2LC68B7167E4F4 New incoming fax message, S8F8E423F9285C5
Incoming fax from +07843-982843 [Fax server]:+07725-855368
Fax ZC9257943991110 New fax message from +07862-678057

Characteristics and Symptoms

Description

On execution, CTB-Locker will then encrypt the files but not limited to the following extensions:
.pdf .xls .ppt .txt .py .wb2 .jpg .odb .dbf .md .js .pl, etc.

After the files have been encrypted successfully by the malware, a pop-up window will appear on the screen, with the countdown time of 96 hours to get the decrypted files back and some other details as shown below:

Please be informed that we have strengthened our McAfee Antivirus with the necessary software patches, however, request you to avoid situations by not opening suspicious emails and attachments (using your official or personal emails).

Please report to IT at it-helpdesk@del.amarujala.com if you come across such emails in your inbox.

Regards,

Corp IT Team