Rapid 2.0 Ransomware

Early Alert Report

INTRODUZIONE

In data 25 Marzo 2018 è stata identificata una nuova variante di Rapid Ransomware denominata Rapid 2.0. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto in BTC.

DESCRIZIONE

MD5:

f30747df1db164d104187c52486f15da

E-mail legata al Ransomware:

- supp1decr@cock.li
- supp2decr@cock.li

FUNZIONAMENTO

Rapid 2.0 esegue la crittografia dei file e ne modifica l'estensione in .FRTGH (5 caratteri random).

- **ES:** <File_name>.GQKYO.<extension>
- **ES:** <File_name>.GJLLW.<extension>
- **ES:** <File_name>.JFCWF.<extension>

Successivamente viene creato il file della nota di riscatto che presenta il seguente testo:

- ALL YOUR FILES ARE ENCRYPTED BY RAPID 2.0 RANSOMWARE -
Dont worry, you can return all your files!
Attention!
All your files documents, photos, databases and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase a Rapid Decryptor.
This software will decrypt all your encrypted files and will delete Rapid from your PC.
To get this software you need write on our e-mail:
1. supp1decr@cock.li
2. supp2decr@cock.li (if first email unavailable)
What guarantees do we give to you?
You can send one of your encrypted file from your PC and we decrypt him for free.
But we can decrypt only 1 file for free. File must not contain valuable information
Attention!
Dont try to use third-party decryptor tools because it will destroy your files.