Vurten Ransomware

Early Alert Report

INTRODUZIONE

In data 3 Aprile 2018 è stato identificato un nuovo Ransomware denominato Vurten. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto pari a $10000 in Bitcoin.

DESCRIZIONE

MD5:

f2be597fc76acc3390ff4cf944008ba5

E-mail legata al Ransomware:

vurten_knyert@protonmail.com

Indirizzo Bitcoin:

1Ln9RxSRuDqqFhCTuqBPBKRMeyhVhRaUG4

FUNZIONAMENTO

Vurten esegue la crittografia dei file e ne modifica l'estensione in .improved.

ES: <File_name>.<extension>.improved

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

Your entire network sensetive data was encrypted with our strong algorithm. To recover your data send $10000 to the bitcoin address: 1Ln9RxSRuDqqFhCTuqBPBKRMeyhVhRaUG4 If you do not send money within 7 days, payment will be increased double. After payment you will receive decryption software. Contact email: vurten_knyert@protonmail.com