RansomAES Ransomware

Early Alert Report

INTRODUZIONE

In data 8 Maggio 2018 è stato identificato un Ransomware che esegue la crittografia dei file denominato RansomAES. Il Ransomware offre poi la chiave di decodifica attraverso il pagamento di un riscatto in BTC.

DESCRIZIONE

MD5:

2b745e0a8dadac6b2beccd26ddb8c08d

E-mail legate al Ransomware:

- fbgwls245@naver.com
- powerhacker03@hotmail.com

FUNZIONAMENTO

RansomAES esegue la crittografia di numerosi file sul computer della vittima modificando l'estensione in .RansomAES.

ES: <File_name>.<extension>.RansomAES

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

> All your files are encrypted! Your files are encrypted! They received an extension: .RansomAES Write on our email and we will repair them. fbgwls245@naver.com or powerhacker03@hotmail.com decryption Cost Bitcoin ***. The price depends on how you are using it for us. After *** We will provide decryption tools that help decipher all files. Copy your personal identifier on the document and send it to our email.