MOLE66 Ransomware

Early Alert Report

INTRODUZIONE

In data 2 Aprile 2018 è stata identificata una nuova variante di CryptoMix Ransomware denominata MOLE66. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto in BTC.

DESCRIZIONE

MD5:

c3294c90474063dfb0d28ef8a693a6cb

E-mail legata al Ransomware:

alpha2018a@aol.com

FUNZIONAMENTO

MOLE66 esegue la crittografia dei file e ne modifica l'estensione in .MOLE66.

ES: <File_name>.<extension>.MOLE66

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

!!!All your files are encrypted!!! What to decipher write on mail alpha2018a@aol.com Do not move or delete files!!!! ---- Your ID: (Personal-ID)-****-****-f3a91818cea7 ---- !!! You have 3 days otherwise you will lose all your data.!!!