Thanatos Ransomware

Early Alert Report

INTRODUZIONE

In data 18 Febbraio 2018 è stato identificato un nuovo Ransomware denominato Thanatos. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto pari a 0,01 Bitcoin.

DESCRIZIONE

MD5:

681211a7b964eaffd13e0610d82a25e7

Indirizzo Bitcoin:

1DRAsxW4cKAD1BCS9m2dutduHi3FKqQnZF

E-mail legata al Ransomware:

c-m58@mail.ru

FUNZIONAMENTO

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

ES: <File_name>.<extension>.THANATOS

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

Your computer is encrypted. The BE data will of the All the lost the if you do not a pay 0.01 The BTC to the specified 'The BTC wallet 1DRAsxW4cKAD1BCS9m2dutduHi3FKqQnZF the after payment you will of the receive the decryption below code from the this mail c-m58@mail.ru