Heropoint Ransomware

Early Alert Report

INTRODUZIONE

In data 6 Gennaio 2018 è stato identificato un nuovo Ransomware denominato Heropoint. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto pari a $20 in BTC.

DESCRIZIONE

MD5:

dfa8129b30f1340fd912c6492069777b

E-mail legata al Ransomware:

Heropointyt@gmail.com

FUNZIONAMENTO

Il Ransomware esegue la crittografia di numerosi file e ne modifica l'estensione in .(serie numerica random).

ES: <File_name>.<extension>.325727331838

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

the WHAT HAPPENED? Your precious files have been encrypted from my virus How do i adjust this? Pay 20 in bitcoin to $ password the get the WHAT the DO the NOT HAVE to the TO the DO? The task manager Have the Open the Open the cmd (command the prompt) the Open Regedit and sethc ..... the Run of pc in Safe-Mode the Delete rigestries msconfig from the WHAT of IT of DOES HAPPEN the IF I of the DO the NOT PAY? Well .... to files, photos, texts , word / powerpoint projects you can say goodbye ...