SERVER Ransomware

Early Alert Report

INTRODUZIONE

In data 4 Gennaio 2018 è stata identificata una nuova variante di CryptoMix Ransomware denominata SERVER. Il Ransomware esegue la crittografia dei file offrendo poi la chiave di decodifica attraverso il pagamento di un riscatto in BTC.

DESCRIZIONE

MD5:

d0c47bd4b16f5c77ef114004b6b464b0

E-mail legate al Ransomware:

serverup@keemail.me serverup@protonmail.com serverup1@yandex.com serverup3@yandex.com ann.c@iname.com

FUNZIONAMENTO

SERVER esegue la crittografia di numerosi file e ne modifica l'estensione in .SERVER.

ES: <File_name>.<extension>.SERVER

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

Hello! Attention! All Your data was encrypted! For specific informartion, please send us an email with Your ID number: serverup@keemail.me serverup@protonmail.com serverup1@yandex.com serverup3@yandex.com ann.c@iname.com Please send email to all email addresses! We will help You as soon as possible! IMPORTANT: DO NOT USE ANY PUBLIC SOFTWARE! IT MAY DAMAGE YOUR DATA FOREVER! DECRYPT-ID-[id] number