If it sounds too good to be true, it most likely is: Nobody can decrypt the Dharma ransomware

By Gareth Corfield

Published: 2019-11-11 · Archived: 2026-04-02 11:31:17 UTC

A data recovery company is dubiously claiming it has cracked decryption of Dharma ransomware – despite there being no known method of unscrambling its files.

Infosec researcher Brett Callow of Emsisoft had a little fun trying to replicate Emsisoft's exposure of ransomware middleman company Red Mosquito Data Recovery earlier this year, now he has turned his attention in another direction.

Australian biz Fast Data Recovery boasted that it is capable of decrypting Dharma, which data recovery biz Coveware's chief exec Bill Siegel described as implying "they have tools and computing power beyond that of the NSA".

"If this was the case, they would sell their technology for millions, if not billions, rather than using it to help small businesses," he added.

Callow posed as a customer (having borrowed his wife's business email address, with her consent) while contacting Fast Data Recovery, asking if the firm could decrypt encrypted files that mentioned the word Dharma. What Callow had done was encrypt the files himself.

He got back a standard auto-reply email:

That was followed up with an offer to carry out a "server prevention and network security audit" at AU$750 per server and $120 per PC – with a discount to $70 if one had more than 10 PCs.

Michael Gillespie, creator of ID Ransomware, opined: "There is no way to 'reverse engineer the ransomware decryption key' for Dharma. The encryption is perfectly implemented, and it's simply not possible. The only way to recover files encrypted by Dharma is with the ransomware dev's key. Any company which claims it can recover files by other means is almost certainly just paying the ransom."

When Emsisoft's Callow didn't reply to the quote, Fast Data Recovery tried again:

At this point, Callow broke off contact with the firm, but the case smells similar to other companies claiming to be able to decrypt ransomware when all they do is act as a middleman, taking money on the pretence of "decrypting" ransomware, then paying the ransom and in turn banking a margin for doing so.

The most outrageous case aside from Red Mosquito (as mentioned above) was Dr Shifro, a Russian firm that also claimed to be able to decrypt Dharma. This turned out to be one Belarusian man who had made around £300,000 from taking Bitcoin payments while negotiating with ransomware authors.

Emsisoft's CTO, Fabian Wosar, concluded: "Since emerging in 2016, Dharma has been reverse engineered to death by the entire malware research community. If a flaw existed that enabled the encryption to be broken, it would almost certainly have been discovered a long time ago. To break Dharma within any of our lifetimes without having discovered a flaw would require access to a quantum computer that is capable of running Shor's algorithm. The highest number ever factorized using said algorithm and quantum computers is 21, which is just short of the 307 digits that would be required to break Dharma."

Sometimes, these types of services really are too good to be true.

Fast Data Recovery has been asked for comment. ®
