Subject: IGAL encrypted folder
Posted by idkfa46 on Tue, 29 Dec 2020 13:49:08 GMT
View Forum Message <> Reply to Message

Hi guys,
my upp folder has been encrypted by IGAL ransomware virus.
In your opinion is there any chance to find out the decryption key comparing a couple of files I have in both versions encrypted and not encrypted?

Thanks

Subject: Re: IGAL encrypted folder
Posted by Xemuth on Thu, 31 Dec 2020 10:02:02 GMT
View Forum Message <> Reply to Message

Hello idkfa46,

My knowledge about this kind of soft are extremely limited so don't take my speak for truth !

In my opinion it wont really help you.
To crack this kind of software you need algorithm used to encrypt. in your case, if you know the algorithm you can still try to create a quickprogram that decrypt your file with a random key then if the hash of your file match with the original one then you have decryption key. On the paper this way of working will always work but in reallity if IGAL use an encryption algorithm based on key with a minimun size of 256 bit then it gonna be impossible to find the decryption key by using bruteforcing.

Quote:Even if you use Tianhe-2 (MilkyWay-2), the fastest supercomputer in the world, it will take millions of years to crack 256-bit AES encryption.

Again, I'm far from being an expert and my knowledge is highly limited.

Subject: Re: IGAL encrypted folder
Posted by idkfa46 on Sat, 02 Jan 2021 16:31:13 GMT
View Forum Message <> Reply to Message

I think you are true... decryption with an online ID seems to be impossible at the moment!

What is a good back-up solution to prevent this kind of data loss? As far as I understood this kind of virus affects the overall SDD, USB external drivers connected, and the cloud storage too...

Best,
Matteo

Subject: Re: IGAL encrypted folder
Posted by Zbych on Sat, 02 Jan 2021 20:24:30 GMT
View Forum Message <> Reply to Message

> idkfa46 wrote on Sat, 02 January 2021 17:31
> What is a good back-up solution to prevent this kind of data loss? As far as I understood this kind of virus affects the overall SDD, USB external drivers connected, and the cloud storage too...

Any backup that has version control (GIT, SVN) or rights management (no right to change uploaded files - GCP).