Still think you can negotiate with REvil and get your files back? Read this first. - DataBreaches.Net

Published: 2021-07-01 · Archived: 2026-04-09 02:19:38 UTC

The government and professionals involved in ransomware incident response have often advised victims not to pay the ransom because even if you pay, you may not get your data back, and you may not get your data deleted by criminals who pinky swear that they will delete it. Then, too, they may pinky swear that they will never attack you again or misuse the data they stole from you, but we've also seen that happen.

But if you need another reminder of why *not* to pay, the following chat log contains excerpts from a recent chat involving a victim who paid REvil, who had promised them a decryptor key, support, and a file tree of all the files REvil had exfiltrated.

After you read the excerpts below, ask yourself whether you think REvil was lying in this interaction when they claimed they had exfiltrated data or whether they were lying later when they claimed that they hadn't exfiltrated data. And if you don't know what to believe, what would you do if you find yourself in the victim's situation next week?

Either way, REvil inflicted self-injury to their reputation by showing that their word could not be relied upon.

The initial demand in the incident below was for $50,000. After some negotiations, it was down to $25,000

> […]
>
> Victim: OK, let me talk to my boss and get back to you.
>
> Victim: Just so I'm clear that payment would get us a decryptor for all our encrypted computers?
>
> *REvil Support: of course*
>
> Victim: OK we are working on getting the money together right now. Did you take any files from our computers? And how fast after we pay could we get the decryption software?
>
> *REvil Support: few minutes*
>
> Victim: OK thats good to know but my boss still wanted to know about whether or not you guys took our data before we sent the money.
>
> *REvil Support: We took your data*
>
> Victim: What did you take?
>
> *REvil Support: It will take more than a month to analyze the data. If all you need is a data, leave this chat.*

> Victim: We still want to move forward with payment for the decryptor we are just trying to understand what data was taken because it could impact our customers and we care about them. If you can give us a list of files it would help us a lot. Can you confirm that the bitcoin wallet is still [redacted]? Will you help us if something goes wrong with the decryption?
>
> Victim: We want to make payment today if you can confirm the wallet for us. We don't want to send it to the wrong place.
>
> *REvil Support: [wallet redacted] yes it is the right adress*
>
> Victim: thanks for verifying.
>
> Victim: we are getting ready to make payment. Are you able to provide us a Dir listing of what you exfil'd?
>
> *REvil Support: of course*
>
> […]
>
> Victim: OK we sent the 0.77 Bitcoin, please confirm as soon as you get it.
>
> *REvil Support: confirm*
> *REvil Support: yes for all network*
> *REvil Support: waiting 3 confirmations*
>
> Victim: We are trying to decryption tool now. You said before you would provide us with a directory listing of the files you took. Can you send that now?
>
> Victim: We are trying to decrypt systems but you guys changed our domain admin password and we can't get any further without that. Can you tell us what you changed it to?
>
> *REvil Support: wait for answer*
>
> Victim: Did you find the password? We can't decrypt some systems without it.
>
> *REvil Support: wait for answer*
>
> *REvil Support: 123456seX*
>
> Victim: That worked thank you. We are still decrypting some of the systems. Do you have a directory listing of the files you took in the meantime?
>
> *REvil Support: We did not take any data from you*

So REvil lied — either when they claimed they had exfiltrated data or when they claimed they hadn't.

DataBreaches.net reached out to the company that we think may have been the victim, but the only response received so far was an auto response (no pun intended) offering us a great warranty on a car purchase.

As a reminder, REvil has previously made clear that they do *not* give victims any of their data back at all. They claim that doing that would violate their privacy policy, but they will give paying victims a file tree showing what was allegedly exfiltrated.

Of course, how would a victim know that REvil didn't just take a screencap of a directory and grab a few files for proof? Perhaps victims who are tempted to pay ransom because they fear that REvil exfiltrated their files should demand substantial proof of that claim — more than just a handful of files posted as proof of claim.

Source: https://www.databreaches.net/still-think-you-can-negotiate-with-revil-and-get-your-files-back-read-this-first/