

Forum:[Hack Forums](#)

Thread: [Ransom Ware](#)

Daddy???????????? - May 31, 2017, 2:52 pm

So basically our server machine was infected and all the files are encrypted, backups are gone, everything is basically fucked at this point.

Since all the files are encrypted, they left three emails and I can't find shit anywhere else for them, they want 1 Bitcoin for all the files to be unlocked which I don't have a problem paying but whose to guarantee it will actually happen.

Is there anything I can possibly do at this point?

D?ceived - May 31, 2017, 2:54 pm

It all depends on what ransom ware it is as may have a public decryption tool

Daddy???????????? - May 31, 2017, 2:55 pm

(May 31, 2017 02:54 PM)D?ceived Wrote: [\[CITE\]](#) It all depends on what ransom ware it is as may have a public decryption tool

<https://hastebin.com/eyukunagip.rb>

Encryption for one of the files.

D?ceived - May 31, 2017, 2:56 pm

(May 31, 2017 02:55 PM)Daddy???????????? Wrote: [\[CITE\]](#) <https://hastebin.com/eyukunagip.rb>

Encryption for one of the files.

does it say anywhere a name of ransomware?

Daddy???????????? - May 31, 2017, 2:57 pm

(May 31, 2017 02:56 PM)D?ceived Wrote: [\[CITE\]](#) does it say anywhere a name of ransomware?

Nope, just all the files are encrypted with basically saying email-bestdecrypt@qq.com.ver-CL 1.3.1.0.id-

D?ceived - May 31, 2017, 3:00 pm

(May 31, 2017 02:57 PM)Daddy???????????? Wrote: [\[CITE\]](#) Nope, just all the files are encrypted with basically saying email-bestdecrypt@qq.com.ver-CL 1.3.1.0.id-

hmm tried various searches of the image the encryption and emails etc but cant find anything

Daddy???????????? - May 31, 2017, 3:03 pm

(May 31, 2017 03:00 PM)D?ceived Wrote: [\[CITE\]](#) hmm tried various searches of the image the encryption and emails etc but cant find anything

Looks to be Cryakl Ransomware, tried a tool that Kaspersky has but it's like "Requires original file" Well no shit I wish I had that original file.

D?ceived - May 31, 2017, 3:05 pm

<https://www.pcrisk.com/removal-guides/11220-cryakl-ransomware>

this guide looks to be promising

5chn4pp - May 31, 2017, 3:19 pm

(May 31, 2017 03:03 PM)Daddy????????????? Wrote: [\[CITE\]](#) Looks to be Cryakl Ransomware, tried a tool that Kaspersky has but it's like "Requires original file" Well no shit I wish I had that original file. I think it means you only need 1 or 2 original files, so after that it should figure out all other files.

Daddy????????????? - May 31, 2017, 3:20 pm

(May 31, 2017 03:19 PM)Satudarah Wrote: [\[CITE\]](#) I think it means you only need 1 or 2 original files, so after that it should figure out all other files.

Yeah, I am working on it. Thanks for the help :)

I fucking hope I can get this shit back, then do an instant backup, format, update everything, be good to go.

5chn4pp - May 31, 2017, 3:24 pm

(May 31, 2017 03:20 PM)Daddy????????????? Wrote: [\[CITE\]](#) Yeah, I am working on it. Thanks for the help :)

I fucking hope I can get this shit back, then do an instant backup, format, update everything, be good to go.

How did you get infected? Do you have the original file?

This might help to ID your ransomware:

<https://id-ransomware.malwarehunterteam.com/>

xatt - May 31, 2017, 3:26 pm

Fucking rats man, people who do shit like that should be punished to the fullest extent of law.

Aigrod - May 31, 2017, 3:27 pm

If you were running Ubuntu it might have been this:

<http://news.softpedia.com/news/sudo-vulnerability-patched-in-all-supported-ubuntu-linux-releases-up-date-now-516150.shtml>

So update as soon as possible. And make a backup.

President Morty - May 31, 2017, 4:02 pm

(May 31, 2017 03:26 PM)xatt Wrote: [\[CITE\]](#) Fucking rats man, people who do shit like that should be punished to the fullest extent of law.

?

Rats?

This is a ransomware trojan completely different from a RAT. Unless you meant rat as in an insult.

xatt - May 31, 2017, 4:37 pm

(May 31, 2017 04:02 PM)Primetime Draven Wrote: [\[CITE\]](#) ?

Rats?

This is a ransomware trojan completely different from a RAT. Unless you meant rat as in an insult. I didn't mean the computer term. I use rat a lot for schemers and raskulls.

Daddy????????????? - May 31, 2017, 4:39 pm

welp, tried multiple decryptors, nothing.

Contacted a guy from BleepingComputer which seems to be able to find ways to work on this.

But this is beyond fucking repair it seems. lol