

Forum:[Hack Forums](#)

Thread: [pcap file analyze](#)

davydxan - July 16, 2019, 5:15 am

Hello,

Can somebody help me find something hidden in a pcap file?

If I try to analyze it with Wireshark it does not work it says it's an invalid file, BUT it is a valid pcap file.

Maybe there are some tricks idk

Mr. Robot - July 16, 2019, 5:18 am

What are you trying to find.

davydxan - July 16, 2019, 5:21 am

a hidden thing i don't know either

where can i give you the file?

CyberStrike - July 16, 2019, 5:53 am

Post the file, make sure you are not posting like say information you don't want to be public. This "hidden" thing what do you believe it is exactly? Good chance files can be easily recovered of course if it's https and you have not setup key logging (not a keylogger) to capture the client keys it's pretty much worthless.

davydxan - July 16, 2019, 7:16 am

(Jul 16, 2019 05:53 AM)CyberStrike Wrote: [\[CITE\]](#) Post the file, make sure you are not posting like say information you don't want to be public. This "hidden" thing what do you believe it is exactly? Good chance files can be easily recovered of course if it's https and you have not setup key logging (not a keylogger) to capture the client keys it's pretty much worthless.

It is not a keylogger, it's like a game for a prize.

You should find a hint for the next game.

that's the file : transfer,sh/JrviH/packet.pcap

also virustotal scan :

www.virustotal.com/gui/file/e3c0384d1c01a504d2472b20ed1a05562a5196161187716f7866ed4f37b227a6/detection

I managed to open the file with tcpdump in linux but no clue what is the hint.

Maybe you can help me idk

CyberStrike - July 16, 2019, 7:33 am

(Jul 16, 2019 07:16 AM)davydxan Wrote: [\[CITE\]](#) It is not a keylogger, it's like a game for a prize. You should find a hint for the next game.

that's the file : transfer,sh/JrviH/packet.pcap

also virustotal scan :

www.virustotal.com/gui/file/e3c0384d1c01a504d2472b20ed1a05562a5196161187716f7866ed4f37b227a6/detection

I managed to open the file with tcpdump in linux but no clue what is the hint.

Maybe you can help me idk

I meant logging of keys (

<https://jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/>) . What is the sha256sum of the original file as well as your file? It's important to make sure that the file integrity is there.

I'm guessing it's e3c0384d1c01a504d2472b20ed1a05562a5196161187716f7866ed4f37b227a6

davydxan - July 16, 2019, 7:56 am

(Jul 16, 2019 07:33 AM)CyberStrike Wrote: [\[CITE\]](#) I meant logging of keys (jimshaver.net/2015/02/11/decrypting-tls-browser-traffic-with-wireshark-the-easy-way/) . What is the sha256sum of the original file as well as your file? It's important to make sure that the file integrity is there.

I'm guessing it's e3c0384d1c01a504d2472b20ed1a05562a5196161187716f7866ed4f37b227a6
packet.pcap is the original file we don't know anything about it we have to find ourselves a hint for the next game (it might be a link or a photo or a file we don't know)
noone passed this probe yet

also i have no clue what are you talking about hmm

CyberStrike - July 16, 2019, 8:15 am

(Jul 16, 2019 07:56 AM)davydxan Wrote: [\[CITE\]](#) packet.pcap is the original file we don't know anything about it we have to find ourselves a hint for the next game (it might be a link or a photo or a file we don't know)
noone passed this probe yet

also i have no clue what are you talking about hmm
what exactly are you looking for? Is it just open ended find anything or is it something specific?
Should I know Romanian also?

Edit: Extracting files with chaosreader now .. I'll update if anything interesting.

davydxan - July 16, 2019, 8:37 am

(Jul 16, 2019 08:15 AM)CyberStrike Wrote: [\[CITE\]](#) what exactly are you looking for? Is it just open ended find anything or is it something specific? Should I know Romanian also?

Edit: Extracting files with chaosreader now .. I'll update if anything interesting.
yes romanian exactly did you find something related to it?
also i don't exactly it should be a hint as i said for the next step of the game (which can be a link/file/image we don't know)

(Jul 16, 2019 08:15 AM)CyberStrike Wrote: [\[CITE\]](#) what exactly are you looking for? Is it just open ended find anything or is it something specific? Should I know Romanian also?

Edit: Extracting files with chaosreader now .. I'll update if anything interesting.
we received more hints, in the pcap file should be a pdf and it's something written in it

CyberStrike - July 17, 2019, 11:24 pm

I have not found a pdf as of yet, I ran it through chaosreader and foremost, I guess a hexeditor is

next step.

davydxan - July 18, 2019, 1:14 am

(Jul 17, 2019 11:24 PM)CyberStrike Wrote: [\[CITE\]](#) I have not found a pdf as of yet, I ran it through chaosreader and foremost, I guess a hexeditor is next step.

but if u edit the pcap file with notepad++ you will see that it has some lines which you can find in a pdf too if you edit one with np++

CyberStrike - July 18, 2019, 1:16 am

(Jul 18, 2019 01:14 AM)davydxan Wrote: [\[CITE\]](#) but if u edit the pcap file with notepad++ you will see that it has some lines which you can find in a pdf too if you edit one with np++

Like we are editing what the header of the file to be a pdf? Or is it something else?

davydxan - July 18, 2019, 1:46 am

(Jul 18, 2019 01:16 AM)CyberStrike Wrote: [\[CITE\]](#) Like we are editing what the header of the file to be a pdf? Or is it something else?

There is a hidden pdf in the file if you look with notepad++ it might be encrypted.

If you scroll down you will see some lines with numbers, if you edit a normal pdf file with notepad++ you will see the same lines with numbers but i think numbers are different so you have to somehow make a pdf file of that pcap file.

CyberStrike - July 18, 2019, 1:50 am

(Jul 18, 2019 01:46 AM)davydxan Wrote: [\[CITE\]](#) There is a hidden pdf in the file if you look with notepad++ it might be encrypted.

If you scroll down you will see some lines with numbers, if you edit a normal pdf file with notepad++ you will see the same lines with numbers but i think numbers are different so you have to somehow make a pdf file of that pcap file.

I'll check it out with a hex editor from there I can carve out the pdf (hopefully)