

Forum:[Hack Forums](#)

Thread: [Need help for .dll RE/Malware analysis](#)

Bastille - October 28, 2024, 12:26 pm

I retrieved a tool and I'm pretty sure that it's malicious, one of the DLL has been flagged by VT (more than 50 detections) as a stealer, however I'm unable to understand to what IP / server it's related to

I tried Ghidra, I tried PE-bear, but I'm not really familiar with these tools, I tried to look at strings to see if there is something I could recognize such as IP addresses / commands such as "send", "receive", ... but nothing interesting

If someone could give me few tips / hints I could share the .dll

Thanks mates !

utk_1310 - October 28, 2024, 12:32 pm

Use Sandbox, Network Capture line run dll in safe, isolated environment or in VM with Wireshark. I think so.

Bastille - October 28, 2024, 12:43 pm

(Oct 28, 2024 12:32 PM)utk_1310 Wrote: [\[CITE\]](#) Use Sandbox, Network Capture line run dll in safe, isolated environment or in VM with Wireshark.

I think so.

I need to dedicate a network and a machine for this, don't have enough time right now to setup a VLAN and firewalls rules, I wanted to go with RE/static analysis instead

SIM-5528199 - October 28, 2024, 12:49 pm

Send the dll to me in private messages

Bastille - October 28, 2024, 1:19 pm

(Oct 28, 2024 12:49 PM)SIM-5528199 Wrote: [\[CITE\]](#) Send the dll to me in private messages

(Oct 28, 2024 01:01 PM)m0hx Wrote: [\[CITE\]](#) send it my way ill take a look. include all details u got, from where ,etc.

Thanks for the help guys, .dll sent

SIM-5528199 - October 28, 2024, 1:24 pm

(Oct 28, 2024 01:19 PM)Bastille Wrote: [\[CITE\]](#) Thanks for the help guys, .dll sent

So actually, this isn't even encrypted or anything.. Plopped it into IDA and all of the modules instantly loaded with all of the info, loaded it afterwards into dnspy to check and there is nothing out of the ordinary. The file does some audio handling as far as I can tell and there is nothing else there. Nothing referenced in there that could even remotely hack your PC and no encrypted code or hidden code. Nothing. Open DnSpy and check for yourself, you could even decompile it with JetBrains or dnspy to get the source code for the dll and compile it yourself.

jeannyetal - October 28, 2024, 11:57 pm

If its a known stealer family, there are probably tools already made for extracting C2 configs.

If you can share the hash, I can also take a look at it for you.

Bastille - October 29, 2024, 1:41 am

(Oct 28, 2024 01:24 PM)SIM-5528199 Wrote: [\[CITE\]](#) So actually, this isn't even encrypted or anything.. Plopped it into IDA and all of the modules instantly loaded with all of the info, loaded it afterwards into dnspy to check and there is nothing out of the ordinary. The file does some audio handling as far as I can tell and there is nothing else there. Nothing referenced in there that could even remotely hack your PC and no encrypted code or hidden code. Nothing. Open DnSpy and check for yourself, you could even decompile it with JetBrains or dnspy to get the source code for the dll and compile it yourself.

Thanks ! That's maybe why I didn't find something too, but as I'm not familiar yet with static analysis / RE I wanted to be sure haha

(Oct 28, 2024 11:57 PM)jeannyetal Wrote: [\[CITE\]](#) If its a known stealer family, there are probably tools already made for extracting C2 configs.

If you can share the hash, I can also take a look at it for you.

When I ran it on VT it was identified as a well known stealer but it seems that the .dll itself is not malicious, 2 people confirmed it to me, it's probably just used with other malicious artefacts and has been flagged because of this, thanks tho !

SIM-4982069 - November 4, 2024, 9:52 pm

I could take a look too, pm me.

sk009900 - January 5, 2025, 2:24 pm

(Oct 28, 2024 12:49 PM)SIM-5528199 Wrote: [\[CITE\]](#) Send the dll to me in private messages
hi can you please pm me i have some questionss