

Forum:[Hack Forums](#)

Thread: [Malware closing](#)

Adam2017 - June 21, 2018, 8:01 am

Hi guys I am following a lab from college on malware analysis,

for some reason when I run the malware immediately after it starts a process for the virus begins but it terminates after about 2 seconds,

following the lab this should not happen,the process should stay executing instead of terminating

I have tried turning windows defender off,turning off the firewall,turning off updates yet it still doesn't work,the reason why I need the process to run is to do dynamic analysis on it,

I am running a windows 7 32 bit virtual machine on virtual box

I can't do the lab if I can't get the malware to run :(

the md5 hash of the malware is a96ac90621818a65f43fc5720ff57ba3,

I followed the lab extracted the file and named it Trojan.Downloader.exe like we were told too but nope no luck.

could anybody please give their opinions on why the file may not be running?

thanks

CyberStrike - June 21, 2018, 9:05 am

(Jun 21, 2018 08:01 AM)Adam2017 Wrote: [\[CITE\]](#) Hi guys I am following a lab from college on malware analysis,

for some reason when I run the malware immediately after it starts a process for the virus begins but it terminates after about 2 seconds,

following the lab this should not happen,the process should stay executing instead of terminating

I have tried turning windows defender off,turning off the firewall,turning off updates yet it still doesn't work,the reason why I need the process to run is to do dynamic analysis on it,

I am running a windows 7 32 bit virtual machine on virtual box

I can't do the lab if I can't get the malware to run :(

the md5 hash of the malware is a96ac90621818a65f43fc5720ff57ba3,

I followed the lab extracted the file and named it Trojan.Downloader.exe like we were told too but nope no luck.

could anybody please give their opinions on why the file may not be running

thanks

Umm ... why would you even have to turn off defender, if your college lab wants malware analysis on a VM and they at some point suggest " Turn off defender if it doesn't work" I'd be suspect of them, also skip md5 hashes you work with sha256, md5 isn't even used in court, cases are thrown out if md5 is used. Also by all means do not ever update that OS, what if malware used a patched exploit now you won't be able to run it. Are you running flareVM or something? What does process hacker show going on? Perhaps new process or another process is injected / hijacked?