

Forum:[Hack Forums](#)

Thread: [Malware analysis](#)

Adam2017 - June 30, 2018, 1:49 pm

Hi guys so as explained before I am a cyber security/digital forensics student in my third year,

we have two different labs both for dynamic analysis of malware in a secured manner,I have set up a windows 7 virtual machine as told by my lecturer,I downloaded all the analysis tools such as procmon,procexplorer,regshot,wireshark etc,

we were giving the malware to run and given the password which is "infected" we had to rename the first file to Trojan.Downloader.exe and run it from the cmd,which I did but before I can even analyse the malware it terminates by itself and leaves no data at all to analyse in datamon,

you could say maybe it is attaching itself to another process but it's not,as I have done this lab on my old laptop(broken now) and it was in plain sight in procexplorer and procmon so we could analyse it.

So I thought to myself well maybe it could be that the firewall is preventing it from running,so I reset the vm back to the last snapshot before I ran the malware.I turned off the malware turned off updates turned off windows defender and tried running it again but no luck the same results,when I execute the malware it just terminates.

so I said to myself I will try the other lab,I decided to get a new windows 7 vm this time turned the updates off immediately(also firewall etc) so the last update was in 2014 so little chance the virus is patched.

I run the new malware(new lab) with the same tools ready to capture it but no luck it still terminates after a few seconds like the other malware(it's not supposed to do that as shown in the lab)

I would be more than grateful if anybody could give me some suggestions,I need to practice these labs in order to pass a practical exam/assignment in August if I don't get it,I wont have enough money to go back to college and repeat and will be a waste of 3 years(4 if you count the repeat year)

thanks all suggestions appreciated.

HangMansheart - June 30, 2018, 2:44 pm

I've had things like this happen when generating and testing my own stubs. The problem I had most of the time was system architecture issues. I take it your vm is WIndows 7 x64?

sophrosyne - July 1, 2018, 4:20 am

It seems like your VM is setup wrong, but I can't see your configuration. Also, are you using the same internet connection as before, when it did work?

CyberStrike - July 1, 2018, 4:46 am

Previous thread on this just so everyone knows roughly what transpired previously it may help shed

some light on what's going on :

<https://hackforums.net/showthread.php?tid=5852279>

Being that it's an exe file, why not put it into a debugger? Does Wireshark show anything having been downloaded? Are there any new processes/threads or child processes/threads?

Do you mind telling us what this malware is, perhaps give us the sha256 and we can see if we get the same issue. Something else after running the malware perhaps dumping the VM's RAM may further illuminate what's going on, perhaps looking at it in volatility

Adam2017 - July 1, 2018, 8:42 am

Hi guys,

I probably should have mentioned it is a 32 bit windows 7 machine well both of them are the first one is windows 7 32 bit sp1 the second one which I tried is windows 7 home basic 32bit not sure if its service pack 1 but it's not been updated since 2014

the sha256 of the malware in question is
c6e2dc65ce5b0e5c5f0e2618ab2bed46d9952733f7bb70eda0640dd65e203dfb

the md5 is a96ac90621818a65f43fc5720ff57ba3

also I must mention the internet settings on the vm is set to nat

thanks

CyberStrike - July 2, 2018, 1:21 am

I usually keep my VM also Windows 7 but pro (<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>) and with FlareVM tools installed on host only, with inetsim or fakenet-ng running. If you need to download say a secondary stage then I can see using NAT this is an older piece of malware circa 2011 btw.

Adam2017 - July 2, 2018, 9:11 am

(Jul 2, 2018 01:21 AM)Sirru5h Wrote: [\[CITE\]](#) I usually keep my VM also Windows 7 but pro (and with FlareVM tools installed on host only, with inetsim or fakenet-ng running. If you need to download say a secondary stage then I can see using NAT this is an older piece of malware circa 2011 btw.
thanks Sirru5h :)

I sent you a reply in pm, hopefully it went through

Adam2017 - July 5, 2018, 8:58 am

(Jul 2, 2018 09:11 AM)Adam2017 Wrote: [\[CITE\]](#) thanks Sirru5h :)

I sent you a reply in pm, hopefully it went through
Hi Sirruh sent another pm

CyberStrike - July 5, 2018, 2:34 pm

(Jul 5, 2018 08:58 AM)Adam2017 Wrote: [\[CITE\]](#) Hi Sirruh sent another pm
Excellent got it I will run it through FLareVM tonight and see what it does.