

Forum:[Hack Forums](#)

Thread: [Sophus Anti Virus](#)

AceHardware - December 11, 2017, 5:37 pm

I'm having a problem with executing an attack on a machine running Sophus Anti Virus. If anyone knows of anyways I can disguise my payload so it cant see it or a way to disable the Anti Virus I would appreciate it.

BACKGROUND INFORMATION: I will be using a USB Rubber Ducky with Twin Duck firmware to launch this attack. I will plug in the device which is carrying my payload and the Ducky will get to work typing in power shell commands to run the exe file. Then this file will give me remote access to the victims computer through metasploit. The machine will be running the Windows 10 operating system and will not have admin rights. CMD is enabled; Task manager is enabled sometimes (note sure why this fluctuates); power shell is enabled.

CyberStrike - December 11, 2017, 6:14 pm

Download sophos and start testing in a VM I would also strongly suggest that you do NOT have a live internet connection, like update sophos and close that connection and wait ~ 2 minutes before seeing the results double check with a ping to say google, triple check. Don't upload to any online scanning service, at most get the hash and see if you can find the hash value.

Next msfvenom does allow for encoding, that will help, use perhaps VEIL AVET or Shellter. Check out SigThief as well and HashClash. What I usually do is generate a custom payload then use that with VEIL or Shellter, works fairly well you will quickly find that Kaspersky will be a pain in the butt. There are multiple things aswell like hyperion which basically messes with the header of the PE to make it look like it has not been encrypted.

AceHardware - December 11, 2017, 6:36 pm

sirru5h thank you a lot for this information but seeing as I'm not that used to encoding files and using the full capability of Kali Linux I have a few questions.

First off I looked at some stuff on HF and found this <https://hackforums.net/showthread.php?tid=5740856> and was wondering if you had a DL cause I posted a MSG a couple days ago and have come up with no response.

Also don't know if it would help you at all but here's a DL to my payload.

WARNING THIS IS A MALICIOUS EXECUTABLE RUN WITH CATION

Also heads up the reason I'm doing this is because one of my friends bet me I couldn't compromise their system because i told him i was going to study to become a pen tester. (Deadline is the end of this week)

CyberStrike - December 11, 2017, 6:50 pm

Yeah I really wouldn't share a payload, some people are seriously lacking common sense. Well check out the tools that I mentioned, more than likely you can get it past his AV. you just test it before hand, get the same version of the target AV and also one thing is don't over encode it, that will set off AV. See this is the thing we don't need a binder or a crypter we have everything we need in Kali and for free.

Edit: @ work we use code signing certs they cost a bit, but it helps on the job.

<https://www.offensive-security.com/metasploit-unleashed/backdooring-exe-files/> (using msfvenom)

<https://www.veil-framework.com/how-to-customize-backdoor-factory-payloads-within-veil/> (veil)

<https://github.com/secretsquirrel/the-backdoor-factory/wiki> (BackDoor-Factory)

<https://www.shellterproject.com/> (shellter)

AceHardware - December 11, 2017, 6:53 pm

Okay thanks I think I understand now (Also thanks for the help on all my other posts you the real MVP).

CyberStrike - December 11, 2017, 7:04 pm

No problem, you know I am here more than anything to help people, anyhow best of luck.

Something else just popped into my head AV's sometimes don't scan files over a certain size you can use something like truncate in linux and pump up a file .