

Forum:[Hack Forums](#)

Thread: [Windows defender detect kali linux payload](#)

tyche90 - March 6, 2019, 6:02 am

Hello guys, just trying to learn some basics about ethical hacking and I have some issues with Windows 10 defender, he is picking up my payload that I create with Kali Linux, on Windows 7 I have no problem as well on any Android device.

Is there any way to bypass that?

I tested this in virtual machine btw.

__Digital__ - March 6, 2019, 12:16 pm

Yes there is a way but you must interact with defender before your payload is executed. Also consider getting your payload to be signed

CyberStrike - March 6, 2019, 3:02 pm

Well this is a lab not sure why you need to run AV but okay. I would simulate an EV signing certificate by generating and importing it into the root trust, then from there I would also sign the executable with that certificate.

PerfectStorm - March 6, 2019, 3:49 pm

Those payloads are probably old as the hills. They are detected much.

Get a RAT.

__Digital__ - March 6, 2019, 4:24 pm

First of all a rat wouldn't matter with defender, if you don't know how to interact with defender you will not bypass it.

tyche90 - March 7, 2019, 12:23 pm

(Mar 6, 2019 05:24 PM) **__Digital__** Wrote: [\[CITE\]](#) First of all a rat wouldn't matter with defender, if you don't know how to interact with defender you will not bypass it.

Could you point me in a good direction with how to interact with it? I would love to learn few things that could maybe help me out to find new job, so far I was working only in Windows OS environment but I find it out to be waste of time.

__Digital__ - March 7, 2019, 4:16 pm

(Mar 7, 2019 01:23 PM) **tyche90** Wrote: [\[CITE\]](#) Could you point me in a good direction with how to interact with it? I would love to learn few things that could maybe help me out to find new job, so far I was working only in Windows OS environment but I find it out to be waste of time.

Look into how to use the windows defender cmdlets and you will figure out how to interact with it and tell it what to do before your payload is executed..