

Forum: [Hack Forums](#)

Thread: [Need help intentionally flagging an exe as malware \(Microsoft Defender Cloud\)](#)

bluu - October 13, 2026, 5:04 am

Have not worked on this type of a project in a while, to turn long to short I'm attempting to find some behavioral actions/patterns that are guaranteed to be detected by Microsoft Defender (cloud delivery), simple stuff that is generally detected and easy to make (unlike a entire malware strain), i have tried grabbing WiFi passwords and sending over internet, not detected apparently and i have not had enough time to test other obvious pieces of malware, i know i could use actual malware samples but i really don't wanna pull up a virtual machine in 2026 just for a fkn test, most miserable shit imaginable, any help is appreciated.

Bastille - October 13, 2026, 5:28 am

Hello, if you just want to trigger Windows Defender check the following

<https://www.eicar.org/download-anti-malware-testfile/>

It's a file flagged as malicious to test EDR and stuff, but it doesn't harm your computer. It's its purpose.

If you want to simulate a malicious activity, you can also check Atomic Red Team :

<https://github.com/redcanaryco/atomic-red-team>

If you just want to add a behavior on an existing program/code that could trigger Windows Defender, the detection is not only based on the behavior, but it also checks things like :

- part of codes used in other malware
- malicious domain name
- malicious IP addresses

Even if you had one behavior that could be associated to a malware, it doesn't guarantee your executable will be considered as a malware, because even things like disabling VSS service and deleting Shadow Copies can be a legitimate action.

Other ideas :

- adding encrypted powershell command-line
- packing with UPX or other packers (change the entropy of the PE)
- adding scheduled task (for persistence)
- adding / editing registry keys (persistence)
- checking for antivirus installation on the machine (enumeration of many AV)
- enumeration of shared folders
- beaconing C2 communication

For other ideas, you can check the following website : <https://attack.mitre.org/>

CL1B - October 13, 2026, 5:36 am

If you want that just click fix with powershell without using any patches beforehand.

There's so many detection vectors in any form of click fix you're bound to trigger it.

From a intellectual viewpoint; closer to exploit = more defender action, closer to human error = little to no defender action.

Defender is and will always be consumer grade, so keep that in mind.

DramaKing - *October 13, 2026, 8:15 am*

Printing WiFi passwords is a legitimate command, so that shouldn't trigger detection. EICAR is good, but a basic keylogger is so simple that it should be easily flagged.

bluu - *October 13, 2026, 11:56 pm*

thank you all for the help and advice, i appreciate yalls effort, one thing, is it actually possible to set off cloud delivery (which bypasses static) via an powershell script? i thought it would just block the command (sends error to terminal) rather than settings off a trigger on cloud, am i wrong?