

Forum:[Hack Forums](#)

Thread: [Demo Video - Scan Windows PE on Mac ~ Cross Platform Malware/AV Scans - Python GUI](#)

Hackers - November 8, 2025, 5:27 am

[Video: https://www.youtube.com/watch?v=xuO_hJnJG5Q]

Here's a quick demo video of the current functionality. ClamAV is not ready in there, but VirusTotal via API and also the internal MacWinPE Scanner will run static analysis on any Windows file provided.

The software is written in Python and in the video you are watching a Mac demonstration.

Enjoy the song, I made it :)

I also generated the whole software a couple weeks ago with AI. I didn't write any code or sing any songs.

ttbr0 - November 8, 2025, 6:46 pm

this is cute, a bit like a mac version of pestudio. the ip, file path, hex strings, malware family and packer detections seem off and could use some improvements.

Hackers - November 9, 2025, 6:29 am

(Nov 8, 2025 07:46 PM)ttbr0 Wrote: [\[CITE\]](#) this is cute, a bit like a mac version of pestudio. the ip, file path, hex strings, malware family and packer detections seem off and could use some improvements.

Yeah, definitely agreed on the file paths, this is still in progress. I still need to fix the internal detections for those, and then move onto ClamAV, and then add more to VirusTotal tab

IP addresses - this is already patched in my current version, it was due to a way too forgiving regex pattern, so I cleaned that up and then added 0-255 range checks as well for it to ensure each IP is valid. I now have to re-add port capabilities to allow for 127.0.0.1:1000 formats.

Filepaths is pulling in extra because of how I'm detecting, so it grabs URLs too.

I can remove that but then it becomes trickier to detect (static at least), but I can figure it out I think. If not I can limit it to absolute paths only.

Little tricky though because /path/to/folder could be part of a URL, and /web/index.html can correspond to a local file path too.

Hex is a complete fluke, needs to be rewritten and actually handle string conversions. Completely forgot I was going to kill that tab before demo video

I also want to improve what I am looking for to flag suspicious APIs to make that more robust and not have false-flags.

On malware family, that's technically accurate but needs improvement probably.

I support a few family categories but I ran through a few tests a few mins ago and my rootkit definition is too vague and the trojan family detection is also too vague. It's not incorrect, but the logic I use in the code needs to be updated so that 1 category doesn't override a sub-category when

the sub-category is way more specific & accurate.

Thanks for feedback, I do need to decide what I want to pursue or not. For example clamav and VT could be used for the malware family definitions very reliably, and then I could focus more on the filepath, IP, and other detections to really make the program useful.

Any other ideas for what features you think I should support? Static analysis only for the internal scanner :)

nanipoonani - November 9, 2025, 8:23 am

nice work man
also nice song

Hackers - November 9, 2025, 8:28 am

(Nov 9, 2025 09:23 AM)nanipoonani Wrote: [\[CITE\]](#) nice work man
also nice song

Thanks man, I wrote the lyrics and then entered them into Suno. I tweaked the settings for styles and levels and then edited part of it in their editor

I need to fix some things still but overall, wasn't too difficult to get it to this point

nanipoonani - November 9, 2025, 11:45 am

(Nov 9, 2025 09:28 AM)nodes Wrote: [\[CITE\]](#) Thanks man, I wrote the lyrics and then entered them into Suno. I tweaked the settings for styles and levels and then edited part of it in their editor

I need to fix some things still but overall, wasn't too difficult to get it to this point

i just tried Suno and i am blown away how good it is.

man this AI evolves so fast, AI might be the last human creation

Hackers - November 9, 2025, 12:02 pm

(Nov 9, 2025 12:45 PM)nanipoonani Wrote: [\[CITE\]](#) i just tried Suno and i am blown away how good it is.

man this AI evolves so fast, AI might be the last human creation

Yeah, it can be used for anything

don't need singers, writers, devs, etc for everything created

Now it's about finding new things to create, things AI is not trained on or can't do reliably, like quantum computing, and work with atoms & different things like photons, electrons...

AI gives us the opportunity to focus on what really matters, new technology. We can rely on it also to then take in what we learn, and master it... AI is a progressive concept, we can always train it on new data, so as we learn more, we use AI to automate it as we go.

Spammino - December 2, 2025, 2:45 pm

Thats lit mate

Hackers - December 3, 2025, 8:28 am

(Dec 2, 2025 03:45 PM)Spammino Wrote: [\[CITE\]](#) Thats lit mate
thanks, I think it's cool too :)

I ended up using some of these concepts in another project.

Truthfully, i have 0 need for windows RE/scans right now, but I might revisit this project one day to

finish it. I was really just experimenting at the time.

Tbroker98 - February 16, 2026, 11:35 am

(Nov 8, 2025 06:27 AM)nodes Wrote: [\[CITE\]](#) [Video: https://www.youtube.com/watch?v=xuO_hJnJG5Q]

Here's a quick demo video of the current functionality. ClamAV is not ready in there, but VirusTotal via API and also the internal MacWinPE Scanner will run static analysis on any Windows file provided.

The software is written in Python and in the video you are watching a Mac demonstration.

Enjoy the song, I made it :)

I also generated the whole software a couple weeks ago with AI. I didn't write any code or sing any songs.

bro, the song definetelly gave me headache, why use a song in the video? it was unnecessary, it distracts a lot from the view, but the idea is cool ;)

Hackers - February 16, 2026, 11:38 am

(Feb 16, 2026 12:35 PM)Tbroker98 Wrote: [\[CITE\]](#) bro, the song definetelly gave me headache, why use a song in the video? it was unnecessary, it distracts a lot from the view, but the idea is cool ;)

Eh, it was kind of a 2-in-1 where I made a song and a software in the same hour or so and just put them together.

I hear ya though