

Forum:[Hack Forums](#)

Thread: [Question on detecting common sandboxes](#)

possessed-client - April 27, 2026, 1:46 pm

Can someone please tell me the most effective techniques for detecting sandboxes or point me to relevant resources online, specifically for sandboxes included in VirusTotal, and also some techniques that might work against sandboxing included within popular antiviruses? I know of multiple resources with a lot of techniques discussed like evasions.checkpoint.com or <https://github.com/LordNoteworthy/al-khaser> and a couple others, but they include very many techniques and it'll take some time to figure out a minimal optimal set against target sandboxes. So if it's not a trade secret, any quick suggestions or links that'd set me on the right track?

shir4zz - April 29, 2026, 3:07 am

Here's a list for virustotal related <https://github.com/6nz/virustotal-vm-blacklist>

Also when it comes to things you should check for suspicious machines check RAM, CPU, uptime, mouse movement, idle time, hostnames against popular known, processes, registries for vm entries, vm related files or drivers, screen resolution, disk size, is there a debugger present etc, there's a lot you can check. Most people won't want to share the exact details of what they're using but it's not a trade secret either haha

<https://github.com/kernelwernel/VMAware>

<https://www.youtube.com/watch?v=fFiQhnn3X3U>

Clankered art but the video itself is somewhat good

This is also an interesting read

<https://www.lrq.com/en/cyber-labs/vm-detection-tricks-part-2-driver-thread-fingerprinting/>

possessed-client - April 29, 2026, 7:43 am

(Apr 29, 2026 03:07 AM)shir4zz Wrote: [\[CITE\]](#) Here's a list for virustotal related <https://github.com/6nz/virustotal-vm-blacklist>

Also when it comes to things you should check for suspicious machines check RAM, CPU, uptime, mouse movement, idle time, hostnames against popular known, processes, registries for vm entries, vm related files or drivers, screen resolution, disk size, is there a debugger present etc, there's a lot you can check. Most people won't want to share the exact details of what they're using but it's not a trade secret either haha

<https://github.com/kernelwernel/VMAware>

<https://www.youtube.com/watch?v=fFiQhnn3X3U>

Clankered art but the video itself is somewhat good

This is also an interesting read

<https://www.lrq.com/en/cyber-labs/vm-detection-tricks-part-2-driver-thread-fingerprinting/>

Big thanks, very relevant resources.

Now I'll just need to whittle down to some short set of checks to reduce bloat, detection surface, false positives. And generally I was thinking of trying to not target virtualization itself, since there's

various environments nowadays that are virtualized, but are not for testing and analysis, hence useful to target.

Was thinking of maybe checking disk size, and if there's free space trying to briefly allocate a large chunk - maybe that'd help against the most dumb hooks returning fake values to get Windows to spit out the truth on space. There's probably a lot of other sneaky ways, need to read through the sources, something will probably give inspiration.

shir4zz - April 29, 2026, 8:09 am

Np :)

Also, against reducing bloat and fighting false positives, you shouldn't value all flags at the same level. A good idea would be to implement a confidence level for each flag,, for example what I mean is that hostname shouldn't carry as much weight as, say, having 2 GB of RAM on the box. No real computer should be running with only 2 (hopefully ?) but someone's computer might be named "malware" or "sandbox", it's possible. And yeah that's actually a pretty smart trick to do as they're not ready for you to actually consume space lol