

Forum:[Hack Forums](#)

Thread: [Undetectable keylogger In 2024](#)

mang0123 - June 14, 2024, 12:59 pm

How do you get undetectable keylogger for win10 and win11 in 2024 is it even worth spending time coding an keylogger now bc I know c++ and I planned coding one just don't know how to get it be undetectable and is it even possible and even if I build it undetectable how long will it be like that before I need to change code. I would like someone with knowledge to explain how keylogger work how does it get detected and how to prevent that. Thanks

I cry blood - June 14, 2024, 1:22 pm

When you build organic malware (and the code isn't some copy/paste nonsense) depending how much you spread it, how many people scan it, and what antiviral software analyze it will determine how long it stays FUD. In the end, you'll generally need to either purchase or code your own crypter. Sometimes not even changing the code is enough unless you really rework everything, which is a waste of time in the long run. Some keyloggers are so basic that they don't raise detections. I've written a Windows keylogger in Python that exfiltrates logs to a Discord webhook and it still has yet to be detected by Windows defender. I'm sure it's only a matter of time though.

When you build a keylogger, you're capturing low level key hooks and saving them to a file or storing them within memory, then you're sending them to some sort of endpoint (FTP server, email, Discord, Telegram, IRC, etc). That said, some keyloggers have additional functions, like clipboard logging, screen/webcam capturing, cache/form grabbing, etc. The more routines in your code you add for functionality, the more chance of raising a detection. Also, how the keylogger installs itself is huge. The common local registry start-up keys (Run, RunOnce, etc) are monitored often, as well as Windows Startup directory. The temp folder is heavily analyzed by antiviral software as that's where a lot of programs, malicious or not, unpack files and configurations of all sorts. File size of your binary is equally important. Obfuscation isn't a bad idea. Back in the day, compressing your binary with sometime like UPX helped, but it seems like nowadays certain methods of compression can be identified and actually raise flags more than avoid them.

Some antivirus software will look at the decoded strings in a compiled Windows PE and check for suspicious wording. Some use heuristics to determine the generic actions of a file. Every time said file displays some sort of suspicious property/actions a flag will be raised. After a certain amount of times the file itself becomes flagged and quarantined, if not removed altogether. Machine learning and AI are also being used by certain AV companies to help further this. You'll also need to deal with Windows Smartscreen. That alone can cause enough of a problem.

These are all aspects of what you'll want to consider when building your keylogger. If you have any more questions or if you want me to elaborate on something more please let me know.

DramaKing - June 14, 2024, 1:35 pm

(Jun 14, 2024 12:59 PM)mang0123 Wrote: [\[CITE\]](#) How do you get undetectable keylogger for win10 and win11 in 2024 is it even worth spending time coding an keylogger now bc I know c++ and I planned coding one just don't know how to get it be undetectable and is it even possible and even if I build it undetectable how long will it be like that before I need to change code. I would like someone with knowledge to explain how keylogger work how does it get detected and how to prevent that. Thanks

It will be undetectable from 24-48 hours to a week or more, depending on how many times it gets

scanned, cloud features, and frequency of definition updates.

mang0123 - June 14, 2024, 1:58 pm

(Jun 14, 2024 01:22 PM)I cry blood Wrote: [\[CITE\]](#) When you build organic malware (and the code isn't some copy/paste nonsense) depending how much you spread it, how many people scan it, and what antiviral software analyze it will determine how long it stays FUD. In the end, you'll generally need to either purchase or code your own crypter. Sometimes not even changing the code is enough unless you really rework everything, which is a waste of time in the long run. Some keyloggers are so basic that they don't raise detections. I've written a Windows keylogger in Python that exfiltrates logs to a Discord webhook and it still has yet to be detected by Windows defender. I'm sure it's only a matter of time though.

When you build a keylogger, you're capturing low level key hooks and saving them to a file or storing them within memory, then you're sending them to some sort of endpoint (FTP server, email, Discord, Telegram, IRC, etc). That said, some keyloggers have additional functions, like clipboard logging, screen/webcam capturing, cache/form grabbing, etc. The more routines in your code you add for functionality, the more chance of raising a detection. Also, how the keylogger installs itself is huge. The common local registry start-up keys (Run, RunOnce, etc) are monitored often, as well as Windows Startup directory. The temp folder is heavily analyzed by antiviral software as that's where a lot of programs, malicious or not, unpack files and configurations of all sorts. File size of your binary is equally important. Obfuscation isn't a bad idea. Back in the day, compressing your binary with something like UPX helped, but it seems like nowadays certain methods of compression can be identified and actually raise flags more than avoid them.

Some antivirus software will look at the decoded strings in a compiled Windows PE and check for suspicious wording. Some use heuristics to determine the generic actions of a file. Every time said file displays some sort of suspicious property/actions a flag will be raised. After a certain amount of times the file itself becomes flagged and quarantined, if not removed altogether. Machine learning and AI are also being used by certain AV companies to help further this. You'll also need to deal with Windows Smartscreen. That alone can cause enough of a problem.

These are all aspects of what you'll want to consider when building your keylogger. If you have any more questions or if you want me to elaborate on something more please let me know.

Thank you really good explanation. I can now understand what I am trying to do, also your python keylogger is clever idea did you find it somewhere or was it your own

I cry blood - June 14, 2024, 2:04 pm

(Jun 14, 2024 01:58 PM)mang0123 Wrote: [\[CITE\]](#) Thank you really good explanation. I can now understand what I am trying to do, also your python keylogger is clever idea did you find it somewhere or was it your own

I've heard of people using Discord (via a Discord webhook) as a transport method to submit different data types. For example, [Creal Stealer](#) is a stealer in Python that sends stolen information to Discord. I've also heard of Discord RATs being a thing. I figured if both of those use Discord, then certainly sending keylogs to Discord would be equally as easy, and it was lol. So yeah, I wrote it on my own. I packaged it with [AutoPyToExe](#) which packages Python scripts (and their dependencies) into one executable. Although it worked out, I wouldn't recommend Python, nor using programs like AutoPyToExe for malware. You've got the right idea sticking with Cpp as a coding language. That, and Cpp can also be compiled to either EXE or ELF (if you're using Linux) which gives it not only a speed advantage (since its compiled rather than interpreted, like Python) but someone can't simply right click and view the active code. Cpp also works lower with the system than Python does.

Python funny enough has its own libraries that are capable to hooking keystrokes for you, so you don't really need to know about low level system calls or anything like that. It makes it easy for

people to accomplish their job without doing any heavily lifting. The only issue is, the libraries that are used are more profilable since they're public. It is always best to write your own organic key hook.

bibeqqqq - October 20, 2025, 12:16 pm

(Jun 14, 2024 01:22 PM)I cry blood Wrote: [\[CITE\]](#) When you build organic malware (and the code isn't some copy/paste nonsense) depending how much you spread it, how many people scan it, and what antiviral software analyze it will determine how long it stays FUD. In the end, you'll generally need to either purchase or code your own crypter. Sometimes not even changing the code is enough unless you really rework everything, which is a waste of time in the long run. Some keyloggers are so basic that they don't raise detections. I've written a Windows keylogger in Python that exfiltrates logs to a Discord webhook and it still has yet to be detected by Windows defender. I'm sure it's only a matter of time though.

When you build a keylogger, you're capturing low level key hooks and saving them to a file or storing them within memory, then you're sending them to some sort of endpoint (FTP server, email, Discord, Telegram, IRC, etc). That said, some keyloggers have additional functions, like clipboard logging, screen/webcam capturing, cache/form grabbing, etc. The more routines in your code you add for functionality, the more chance of raising a detection. Also, how the keylogger installs itself is huge. The common local registry start-up keys (Run, RunOnce, etc) are monitored often, as well as Windows Startup directory. The temp folder is heavily analyzed by antiviral software as that's where a lot of programs, malicious or not, unpack files and configurations of all sorts. File size of your binary is equally important. Obfuscation isn't a bad idea. Back in the day, compressing your binary with sometime like UPX helped, but it seems like nowadays certain methods of compression can be identified and actually raise flags more than avoid them.

Some antivirus software will look at the decoded strings in a compiled Windows PE and check for suspicious wording. Some use heuristics to determine the generic actions of a file. Every time said file displays some sort of suspicious property/actions a flag will be raised. After a certain amount of times the file itself becomes flagged and quarantined, if not removed altogether. Machine learning and AI are also being used by certain AV companies to help further this. You'll also need to deal with Windows Smartscreen. That alone can cause enough of a problem.

These are all aspects of what you'll want to consider when building your keylogger. If you have any more questions or if you want me to elaborate on something more please let me know.
hey, you still have that keylogger? could you be able to share it?

DramaKing - October 20, 2025, 1:52 pm

(Oct 20, 2025 12:16 PM)bibeqqqq Wrote: [\[CITE\]](#) hey, you still have that keylogger? could you be able to share it?
What keylogger?

bibeqqqq - October 20, 2025, 2:10 pm

(Oct 20, 2025 01:52 PM)DramaKing Wrote: [\[CITE\]](#) What keylogger?
"I've written a Windows keylogger in Python that exfiltrates logs to a Discord webhook and it still has yet to be detected by Windows defender. I'm sure it's only a matter of time though."
i was talking bout that sentence i also wried a keylogger that sends logs to webhook on discord but its very easy to dectect

DramaKing - October 20, 2025, 2:23 pm

(Oct 20, 2025 02:10 PM)bibeqqqq Wrote: [\[CITE\]](#) "I've written a Windows keylogger in Python that exfiltrates logs to a Discord webhook and it still has yet to be detected by Windows defender. I'm sure it's only a matter of time though."

i was talking bout that sentence i also wried a keylogger that sends logs to webhook on discord but its very easy to dectect

Oh, right. Python scripts are invisible to antivirus. That's why.

bibeqqqq - October 20, 2025, 2:38 pm

(Oct 20, 2025 02:23 PM)DramaKing Wrote: [\[CITE\]](#) Oh, right. Python scripts are invisible to antivirus. That's why.

yea but not mine,do you maybe have some python key logger that is invisible to antivurus and sends webhook on discord?

ilmazingaZ - December 5, 2025, 7:14 am

woooooow insne! i try now