Mini Project in Network Security

Shahd Moslimany

ID: 206813693

This paper addressed to Mr. Doron Ofek: ofekdor@post.bgu.ac.il

Contents

Introduction

Definition of Keyloggers

A keylogger or keystroke logger/keyboard capturing is a form of malware or hardware that keeps track of and records your keystrokes as you type. It takes the information and sends it to a hacker using a command-and-control (C&C) server. The hacker then analyzes the keystrokes to locate usernames and passwords and uses them to hack into otherwise secure systems.

Types of Keyloggers

A software keylogger is a form of malware that infects your device and, if programmed to do so, can spread to other devices the computer comes in contact with. While a hardware keylogger cannot spread from one device to another, like a software keylogger, it transmits information to the hacker or hacking organization, which they will then use to compromise your computer, network, or anything else that requires authentication to access.

Software Keyloggers

Software keyloggers consist of applications that must be installed on a computer to steal keystroke data. They are the most common method hackers use to access a user’s keystrokes.

A software keylogger is put on a computer when the user downloads an infected application. Once installed, the keylogger monitors the keystrokes on the operating system you are using, checking the paths each keystroke goes through. In this way, a software keylogger can keep track of your keystrokes and record each one.

After the keystrokes have been recorded, they are then automatically transferred to the hacker that set up the keylogger. This is done using a remote server that both the keylogger software and the hacker are connected to. The hacker retrieves the data gathered by the keylogger and then uses it to figure out the unsuspecting user’s passwords.

The passwords stolen using the key logger may include email accounts, bank, or investment accounts, or those that the target uses to access websites where their personal information can be seen. Therefore, the hacker's end goal may not be to get into the account for which the password is used. Rather, gaining access to one or more accounts may pave the way for the theft of other data.

What is an example of a keylogger?

A keylogger must be installed inside it or, in the case of a hardware keylogger, physically connected to your computer. There are a few different ways keyloggers attack your device. Via spear phishing, drive-by-download, and via a trojan horse virus.

Implementation:

I decided to implement an executable Keylogger which I spread via a fake

email with the downloadable Keylogger link in it. I used social engineering to

trick the victim that receives my email to click on the link and download and

run my Keylogger. The email that I spread is a replica to an existing email of the Ben-Gurion University Dean (דיקנאט).

The email topic is about the upcoming exam period and about a list of free marathons that are about to be open for some courses for this semester.

The mail contains inside a downloadable link to an application that students can use to register for the relevant marathons, that is the Keylogger.

My goal is to reach as many PCs of students as possible, and to make sure that they download the file, therefore I assume the following preconditions:

- The students pay attention to the mail and read it.
- Shows interest in the application itself and download the attachment.
- Open the application to run it.
- Hopefully the victim does not have a working anti-virus or anti-malware software running in the background.
- Victims PC is connected to the internet for me to receive the keystrokes from him.

Testing, Running and Challenges

Testing the code locally: I have installed python on Windows 10, opened a Cmd with administrator permissions and installed all necessary libraries, specifically email-to, pynput and smtplib using:

- pip3 install email-to pynput smtplib

I created a new fake mail (bgu.dean.2024@gmail.com) for the hacker to receive a mail at the start of the running, then one additional mail every 60 seconds that includes the keystrokes, as long as the code is running.

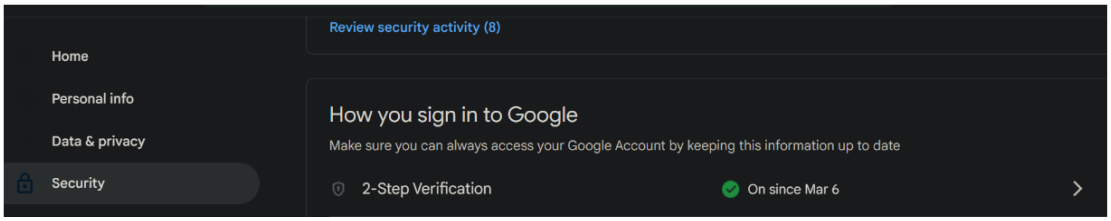
I updated the code and added the fake mail and the main password that I created for the hacker, in order for the code to use it as a receiver for the result.

After running the code for the first time I did not receive the first mail neither any reports, and an error was detected in the Cmd about Gmail authentication and failed to send any mails.

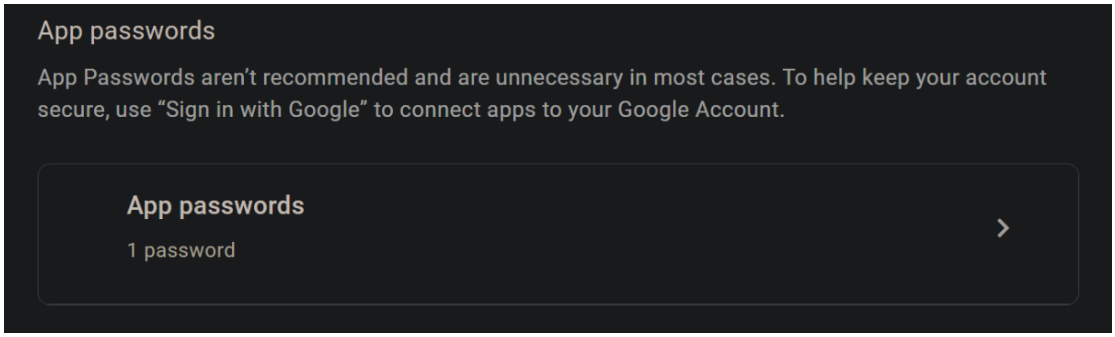
After investigation, The python code sends mails using smtp library, this library was not able to connect via original password and mail.

In order for the information to reach us by email, we must make several configurations in our Gmail:

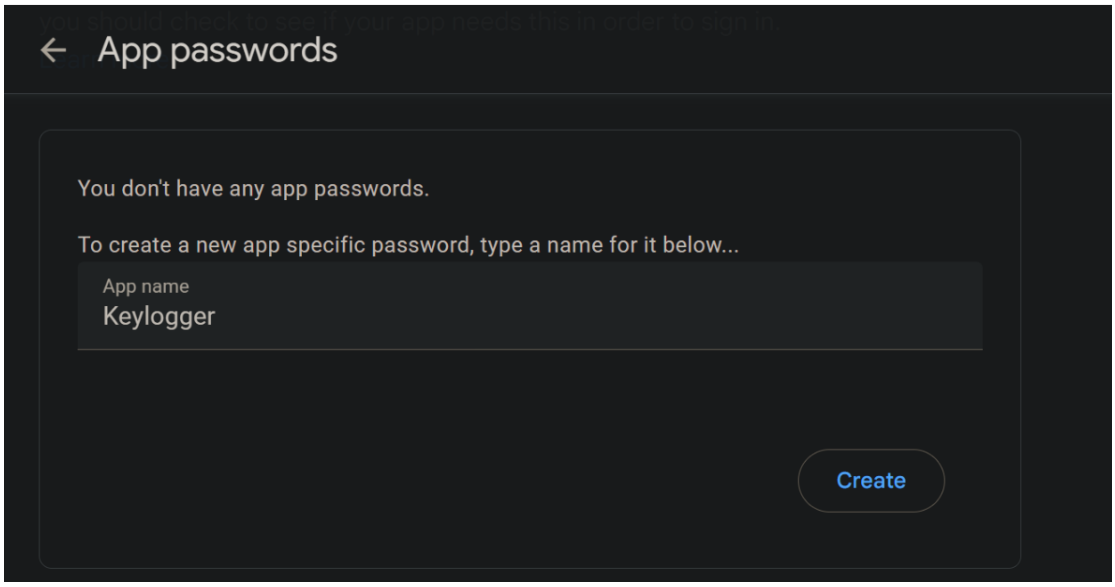
- First, we go to settings, and must activate two-step verification of the account to be able to use the passwords app.



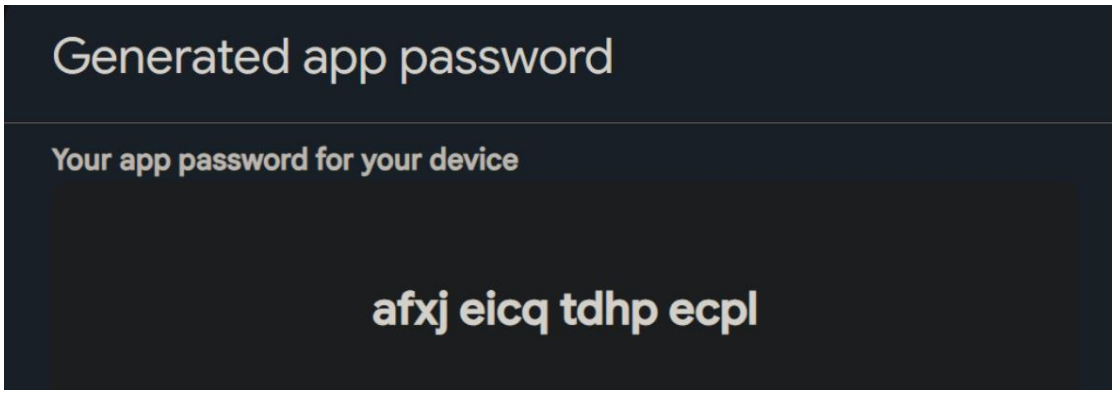
- Once verified, we will search the Apps passwords option.



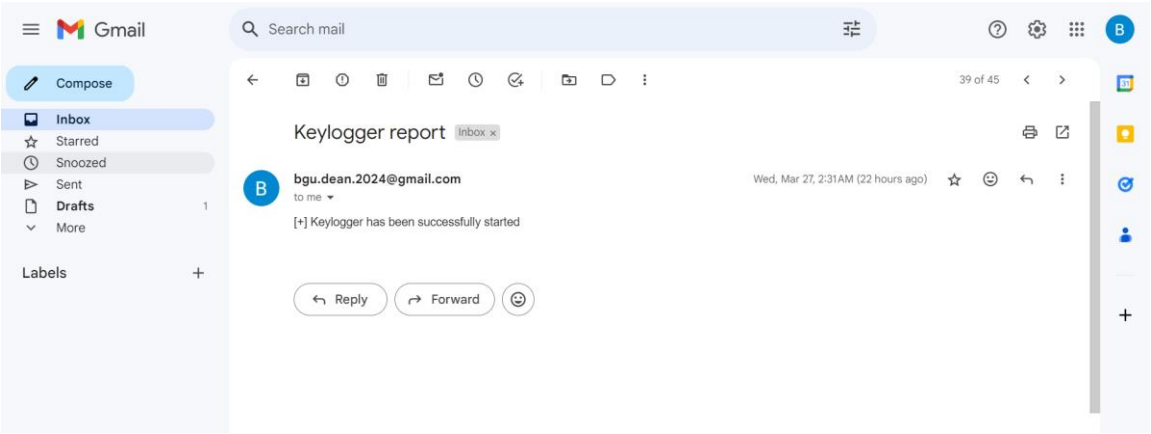
- We give it the name we want.



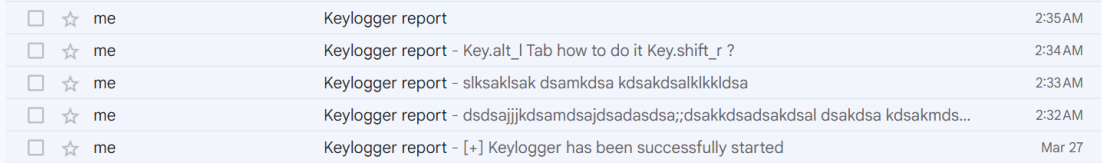
- It will give us a code that we must replace in the part of the script that says "EMAIL_PASSWORD", for example:



I ran the code again and an initial mail was received.



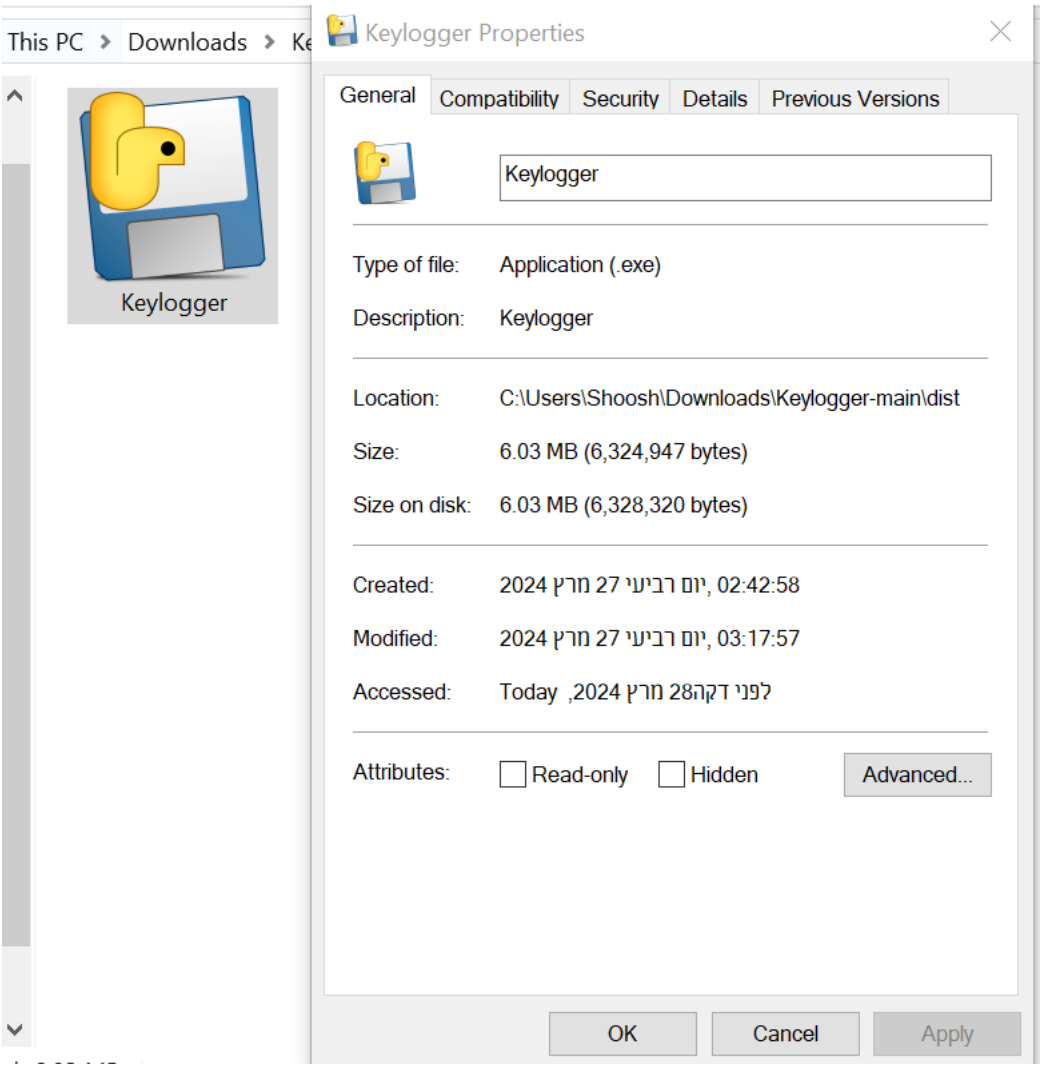
And every 60 seconds a mail was sent with the keystrokes.



After we checked the code locally, and made sure that it works, the next step is to create an executable.

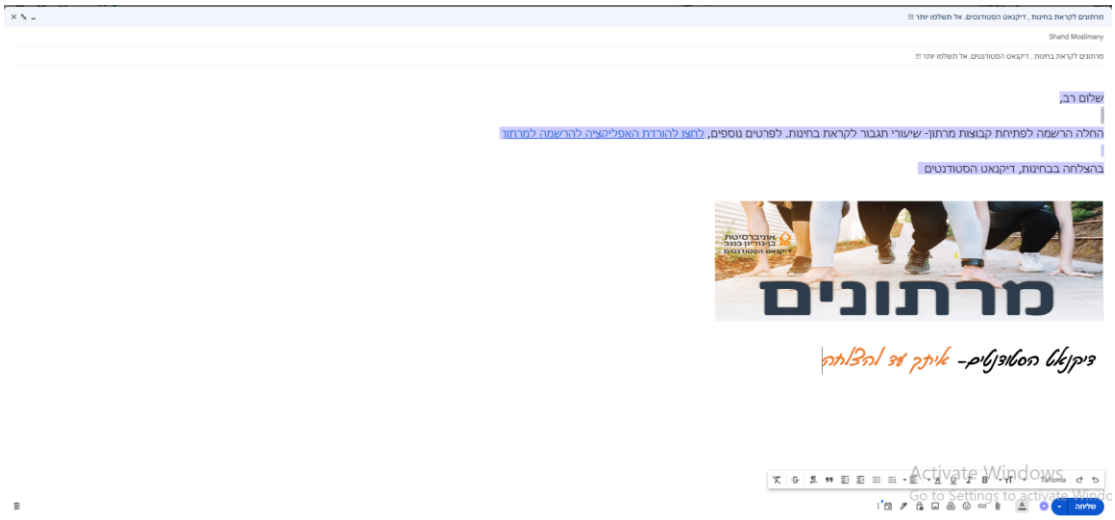
To make it an executable we can use the pyinstaller library by running the following commands:

1. Install the library: pip3 install pyinstaller
2. Create the executable: pyinstaller --onefile --noconsole keylogger.py

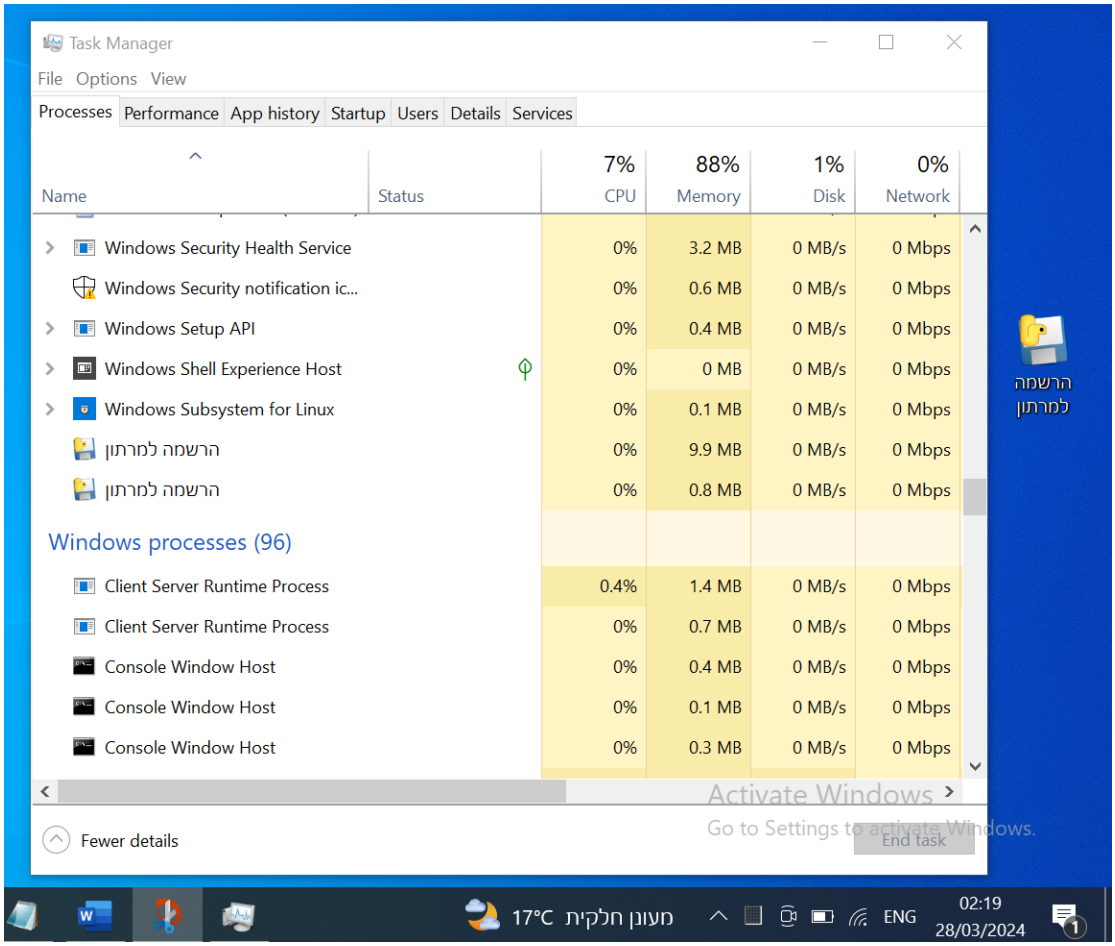


Attack via mail:

I built the fake Email design that is similar to the original one except for the download App instead of a link for the registration.



After downloading the malicious "App" (exe file) and running it, we can see that it is running in the background.



Here we can see that we started to receive reports by mail.

me	Keylogger report - Backspace this is a test		2:22 AM
me	Keylogger report - testing Enter testing Backspace Backspace Backspace Backspace Backspace Backsp...		2:21 AM
me	Keylogger report - Enter Key.ctrl_l fjlhfhfl;kdfjh tes		2:19 AM
me	Keylogger report - [+] Keylogger has been successfully started		2:18 AM

References:

- **Definition of Keyloggers and how it works**
  https://www.fortinet.com/resources/cyberglossary/what-is-keyloggers#:~:text=A%20keylogger%20or%20keystroke%20logger,%2Dcontrol%20(C%26C)%20server.

- **Keylogger instructions and implementation**
  https://github.com/MT-256/Keylogger?tab=readme-ov-file
- **SMTP username and password**
  https://www.youtube.com/watch?v=Y_u5KIeXiVI