MiniProject in Network Security

Egor Stepanishin, ID: 316850395

Yousef Khatib, ID: 318453842

January 29 2020

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

Contents

1 Introduction

What Is A Keylogger Virus ?

Keyloggers are tiny almost invisible applications that creep onto computer easily and record everything from keystroke to clicking model easily.

Once it is through the setting of a PC, it works to send information to the host computer. From the inception of computer virus, users have succeeded to detect the functionality of different viruses and to innovate relevant protection as well. However, it seems a bit difficult, though not impossible, to detect the presence of keylogger so easily. Often referred as Keylogger Trojan, the virus actually is a piece of software that is on use to collect confidential information like bank password numbers, security numbers and credit card details from other computers.

However, it is true that not all keyloggers are malicious but they are hugely being used to do all these odd jobs and it is thus important to know the technique detect this Trojan in detail. Without adequate defense it will be hard to detect this virus and protect information from evil users, who hack your computer from distant places.

Activity:

Keyloggers as a malicious software does different types of jobs. Nowadays, this virus is being sold as commercial software –something that can record its children's online activities or a doubtful spouse may install to keep tabs on the partner. Keyloggers can:

- Record all kind of keystrokes or sometime they are sophisticated enough to run particular activity like tracking web browser. As soon as it observes the desired behavior, keyloggers start working to capture confidential data.

- There are a few websites which attempt to use keyloggers with the purpose to respond to visual cue with the use of mouse, instead of keyword. However, the fact is that some of the Trojans are potential enough to capture screen shot, and easily nullify this strategy of the user.
- This Trojan tends to be the most resolute malware and take extra steps to privatize its presence, including via the use of rootkits

What we Implemented:

We decided to implement an executable Keylogger which we spread via a fake email with the downloadable Keylogger link in it. We use social engineering to trick the victim that receives our email to click on our link and download and run our Keylogger. The email we spread is a replica to an existing email to that of the Ben-Gurion Student Organization (Aguda).

Our email topic is about the upcoming exam period which wishes good luck to all the students and contains inside a downloadable link to an allegedly GPA calculator that is our Keylogger.

Our goal is to reach as many PCs of different students as possible , therefore we assume the following preconditions:

- The student actually pays attention to the mail and reads it.
- Shows interest in the calculator itself and downloads the attachment.
- We assume that the victim has Windows 10 OS , Java SE RTE 8 or above
- 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 us to receive the keystrokes from him.

2 Testing, Running & Compiling the Code

Install dependencies (you need Maven and JDK 8 package installed)

- apt install maven default-jdk default-jre openjdk-8-jdk openjdk-8-jre -y

To generate a .EXE using launch4j are necessary the following packages

- apt install zlib1g-dev libncurses5-dev lib32z1 lib32ncurses6 -y

Go into the repository

- cd sAINT

Install and configure Maven libraries

- chmod +x configure.sh
- ./configure.sh

Run

- java -jar sAINT.jar

Information

- Enter valid Gmail account address (output data email)
- Enter Gmail account password
- Enter character count
- Press Y for lunch4J to generate an EXE file.

Important Note: after all the above is complete , we should have a generated EXE File. Now we must allow ”access to less secure apps” on your Gmail settings page , otherwise Gmail API will block the connection.

3 Code Documentation

3.1 Rules and Processes

The Code (Written in Java) Contains multiple methods all of them are responsible for a sequence of events, What happens is the following(in order):

- We create a new text file in which we store the data.
- The keylogger sequence starts and listens to the keystrokes from the user in the background.
- When we hit the character count number we defined in the settings , an automatic hidden mail is being sent without the host noticing.
- This process continues until a force shutdown is applied to the JAVA RTE or a system reboot.

3.2 Methods documentation

org.jnativehook.keyboard - JNativeHook is a library to provide global keyboard and mouse listeners for Java. This will allow you to listen for global shortcuts or mouse motion that would otherwise be impossible using pure Java. To accomplish this task, JNativeHook leverages platform-dependent native code through Java’s native interface to create low-level system-wide hooks and deliver those events to your application

org.jnativehook.keyboard - Commons-Email aims to provide a API for sending email.

4 Challenges & Difficulties

In the beginning we wanted to do everything in Python/C++ , but after we read more about Keyloggers we found an easier implimention in Java so we decided to do it in Java as well. it was hard in the beginning to set up the environment and install all the neceserry dependencies , After we tested the keylogger localy on the IDE , it was time to generate an executable and test it aswell.

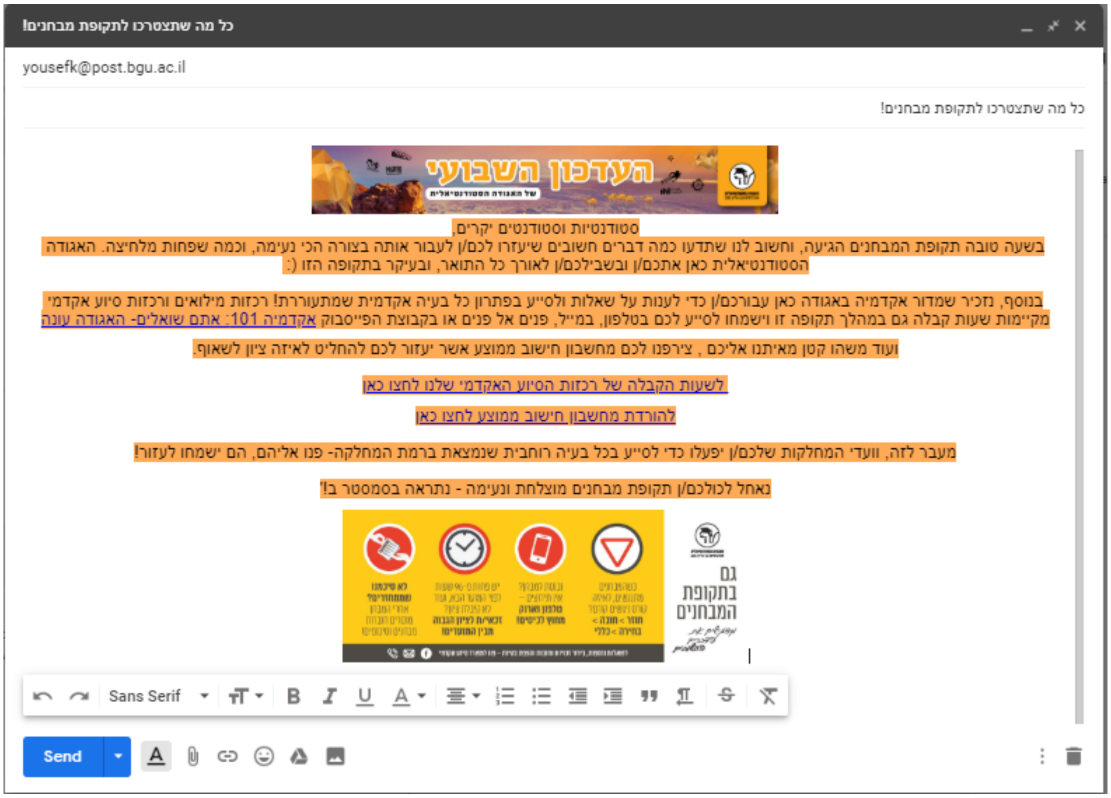
We realized that we needed a fresh new Gmail account for testing so we createrd one, then it was time for RealTime testing but this wasn't easy aswell because the Windows OS has quite a strong anti-virus utility installed.

After bypassing the anti-virus by manually disabling all the security fetures , we executed our keylogger and started hitting all the keys to reach our Character Count . We noticed that everything executed perfectly and was running in the background but we were not receving any email , that was due the fact that google's security polices was blocking 3rd party application to connect to our account for us. This was fixed by enabling the "Access for less secure apps" feture in the google account settings page.

Finally we saw some result , now it was time to construct our fake email. We noticed that attaching the file into the mail was impossible , every technique we tried was cought by the google anti-virus scanner , so we decided to upload it to a 3rd party website and copy a direct download link to it.

5 The Attack Simulation

We did not create another mail that is similar to that of the real Aguda , but we will assume that the receiving side gets the mail from “bgu-aguda@gmail.com” First we start with our fake email design that is 100% original except the 6th and the 8th lines



כל מה שתצטרכו לתקופת מבחנים!

yousefk@post.bgu.ac.il

כל מה שתצטרכו לתקופת מבחנים!

סטודנטיות וסטודנטים יקרים,

בשעה טובה תקופת המבחנים הגיעה, וחשוב לנו שתדעו כמה דברים חשובים שיעזרו לכם/ן לעבור אותה בצורה הכי נעימה, וכמה שפחות מלחיצה. האגודה הסטודנטיאלית כאן אתכם/ן ובשבילכם/ן לאורך כל התואר, ובעיקר בתקופה הזו :)

בנוסף, נזכיר שמדור אקדמיה באגודה כאן עבורכם/ן כדי לענות על שאלות ולסייע בפתרון כל בעיה אקדמית שמתעוררת! רכזות מילואים ורכזות סיוע אקדמי מקיימות שעות קבלה גם במהלך תקופה זו וישמחו לסייע לכם בטלפון, במייל, פנים אל פנים או בקבוצת הפייסבוק אקדמיה 101: אתם שואלים- האגודה עונה

ועוד משהו קטן מאיתנו אליכם , צירפנו לכם מחשבון חישוב ממוצע אשר יעזור לכם להחליט לאיזה ציון לשאוף.

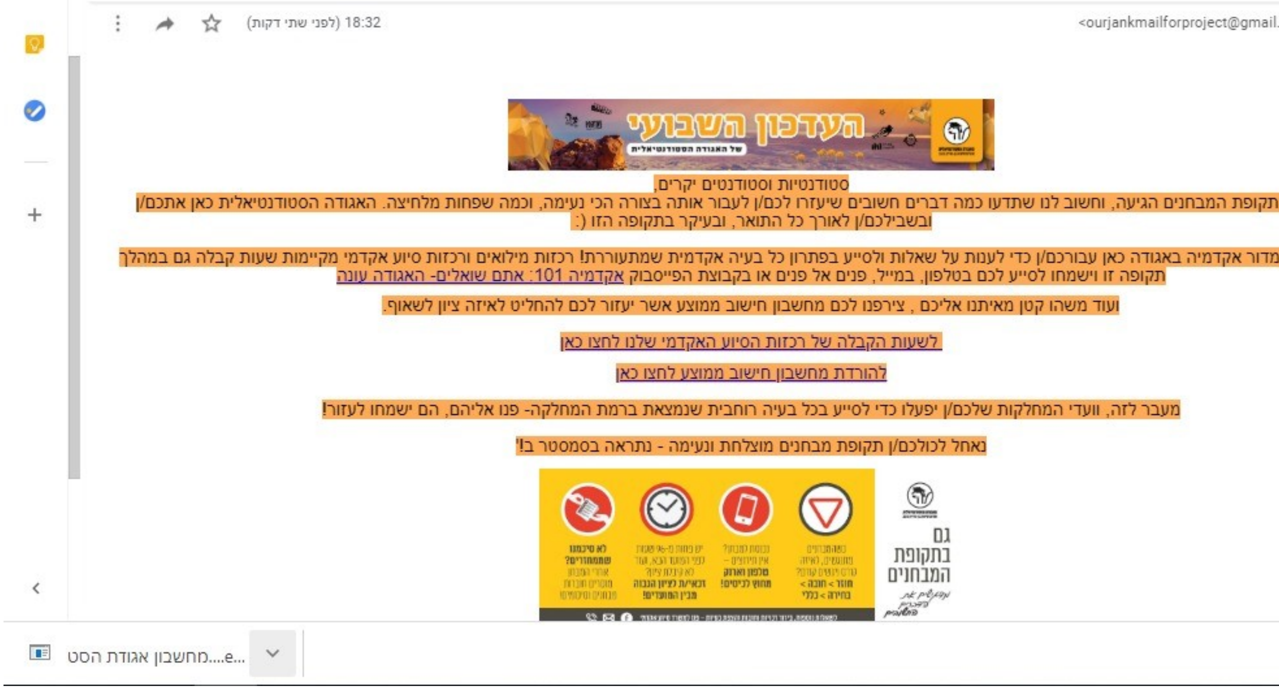
לשעות הקבלה של רכזות הסיוע האקדמי שלנו לחצו כאן

להורדת מחשבון חישוב ממוצע לחצו כאן

מעבר לזה, וועדי המחלקות שלכם/ן יפעלו כדי לסייע בכל בעיה רוחבית שנמצאת ברמת המחלקה- פנו אליהם, הם ישמחו לעזור!

נאחל לכולכם/ן תקופת מבחנים מוצלחת ונעימה - נתראה בסמסטר ב!

Figure 1: The email that we sent



<ourjankmailforproject@gmail.

18:32 (לפני שתי דקות)

סטודנטיות וסטודנטים יקרים,
תקופת המבחנים הגיעה, וחשוב לנו שתדעו כמה דברים חשובים שיעזרו לכם/ן לעבור אותה בצורה הכי נעימה, וכמה שפחות מלחיצה. האגודה הסטודנטיאלית כאן אתכם/ן ובשבילכם/ן לאורך כל התואר, ובעיקר בתקופה הזו :)

מדור אקדמיה באגודה כאן עבורכם/ן כדי לענות על שאלות ולסייע בפתרון כל בעיה אקדמית שמתעוררת! רכזות מילואים ורכזות סיוע אקדמי מקיימות שעות קבלה גם במהלך תקופה זו וישמחו לסייע לכם בטלפון, במייל, פנים אל פנים או בקבוצת הפייסבוק אקדמיה 101: אתם שואלים- האגודה עונה

ועוד משהו קטן מאיתנו אליכם , צירפנו לכם מחשבון חישוב ממוצע אשר יעזור לכם להחליט לאיזה ציון לשאוף.

לשעות הקבלה של רכזות הסיוע האקדמי שלנו לחצו כאן

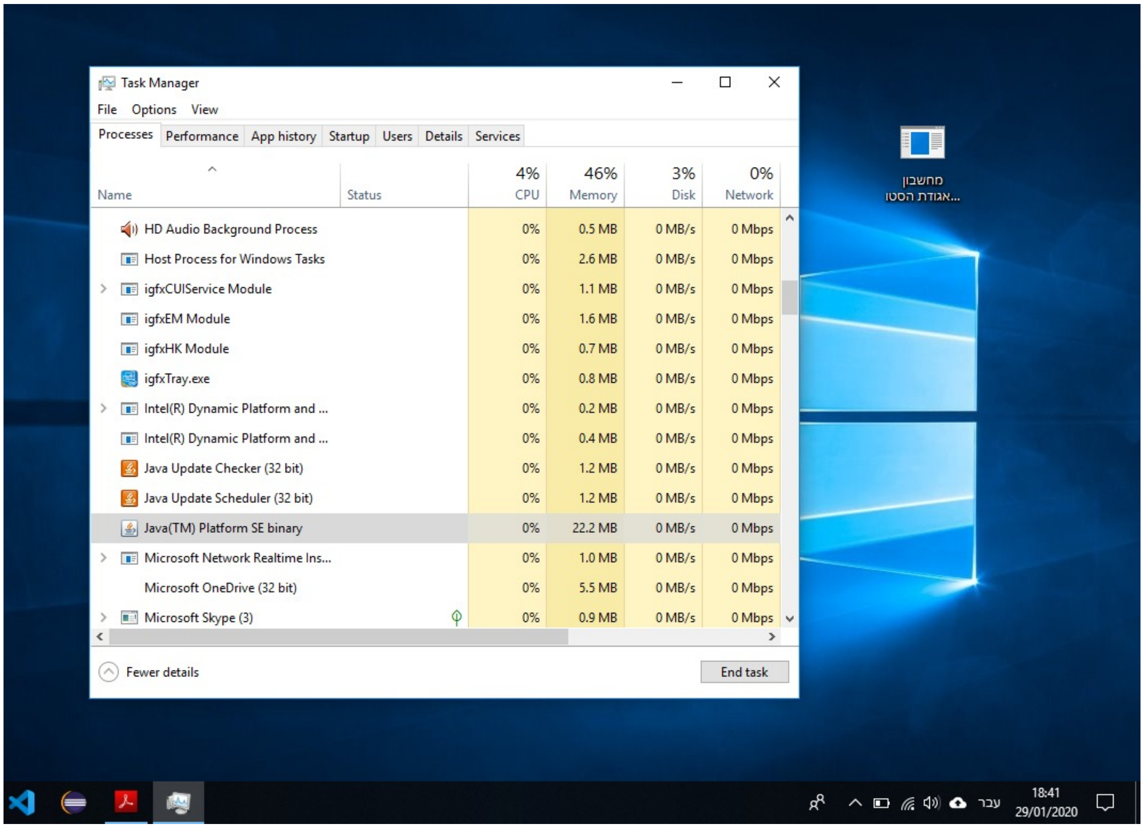
להורדת מחשבון חישוב ממוצע לחצו כאן

מעבר לזה, וועדי המחלקות שלכם/ן יפעלו כדי לסייע בכל בעיה רוחבית שנמצאת ברמת המחלקה- פנו אליהם, הם ישמחו לעזור!

נאחל לכולכם/ן תקופת מבחנים מוצלחת ונעימה - נתראה בסמסטר ב!'

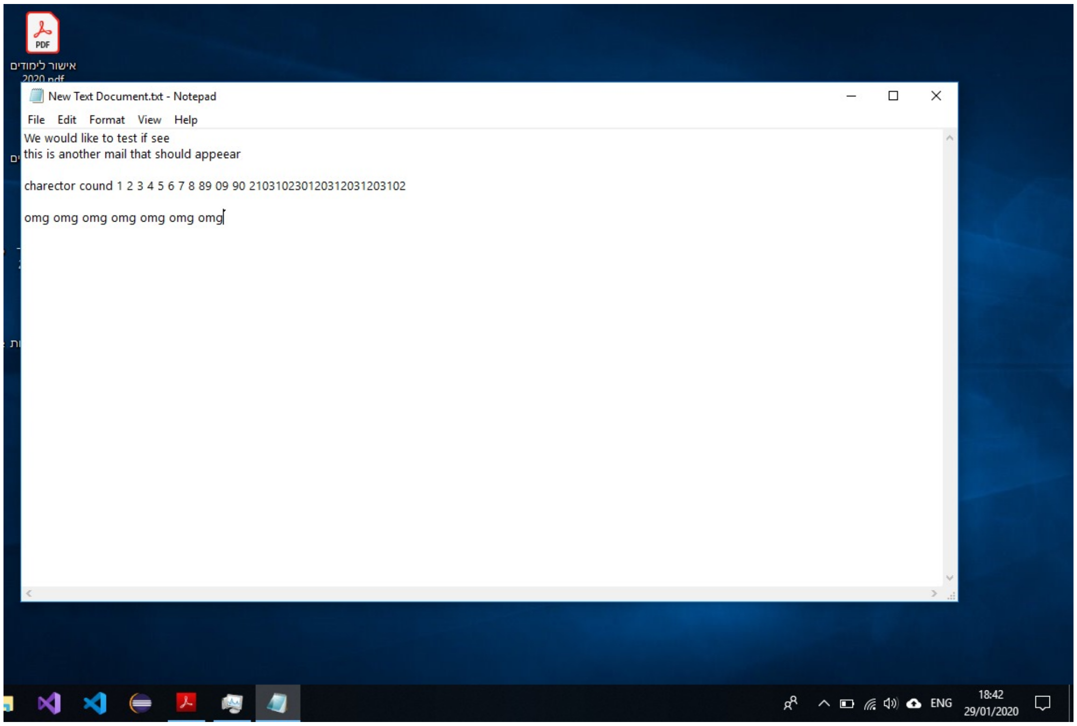
מחשבון אגודת הסט....e

Figure 2: The email as viewed by the victim and the downloaded file



Name	Status	4% CPU	46% Memory	3% Disk	0% Network
HD Audio Background Process		0%	0.5 MB	0 MB/s	0 Mbps
Host Process for Windows Tasks		0%	2.6 MB	0 MB/s	0 Mbps
igfxCUIService Module		0%	1.1 MB	0 MB/s	0 Mbps
igfxEM Module		0%	1.6 MB	0 MB/s	0 Mbps
igfxHK Module		0%	0.7 MB	0 MB/s	0 Mbps
igfxTray.exe		0%	0.8 MB	0 MB/s	0 Mbps
Intel(R) Dynamic Platform and ...		0%	0.2 MB	0 MB/s	0 Mbps
Intel(R) Dynamic Platform and ...		0%	0.4 MB	0 MB/s	0 Mbps
Java Update Checker (32 bit)		0%	1.2 MB	0 MB/s	0 Mbps
Java Update Scheduler (32 bit)		0%	1.2 MB	0 MB/s	0 Mbps
Java(TM) Platform SE binary		0%	22.2 MB	0 MB/s	0 Mbps
Microsoft Network Realtime Ins...		0%	1.0 MB	0 MB/s	0 Mbps
Microsoft OneDrive (32 bit)		0%	5.5 MB	0 MB/s	0 Mbps
Microsoft Skype (3)		0%	0.9 MB	0 MB/s	0 Mbps

Figure 3: After downloading and running the “calculator” we can see that JAVA RTE is running in the background



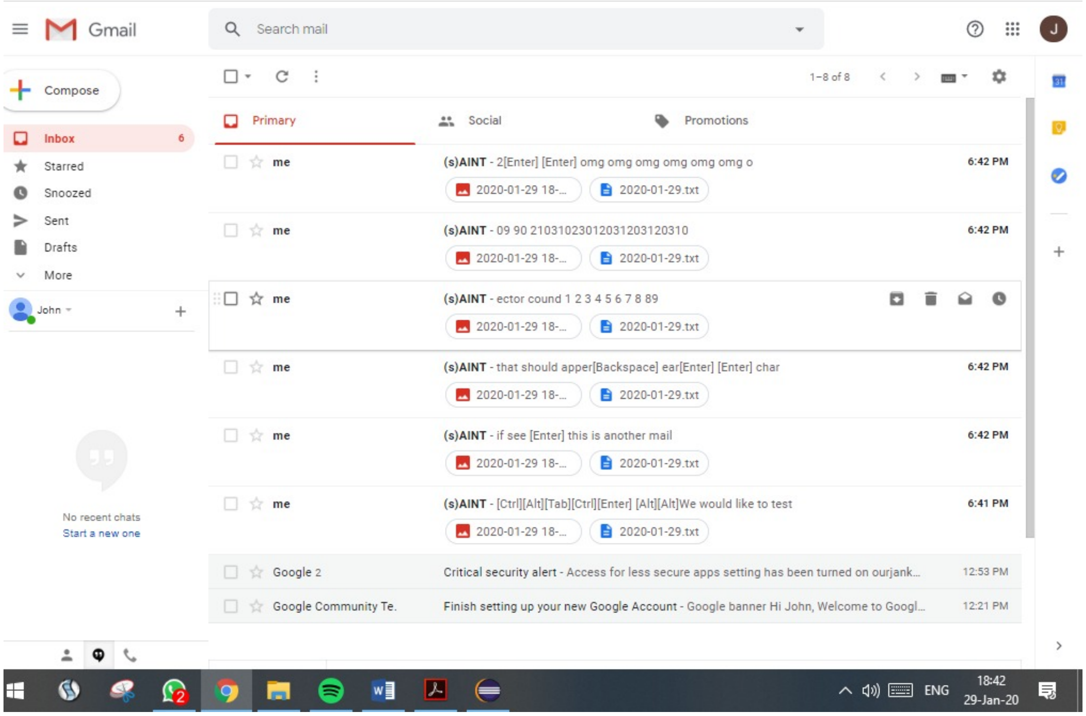
```
We would like to test if see
this is another mail that should appeear

charector cound 1 2 3 4 5 6 7 8 89 09 90 21031023012031203120310 2

omg omg omg omg omg omg omg
```

Figure 4: Testing the key-Strokes (notice the time in the right corner – 18:42)

Character count is 30



me (s)AINT - 2[Enter] [Enter] omg omg omg omg omg omg o 6:42 PM
2020-01-29 18-... 2020-01-29.txt

me (s)AINT - 09 90 21031023012031203120310 6:42 PM
2020-01-29 18-... 2020-01-29.txt

me (s)AINT - ector cound 1 2 3 4 5 6 7 8 89
2020-01-29 18-... 2020-01-29.txt

me (s)AINT - that should apper[Backspace] ear[Enter] [Enter] char 6:42 PM
2020-01-29 18-... 2020-01-29.txt

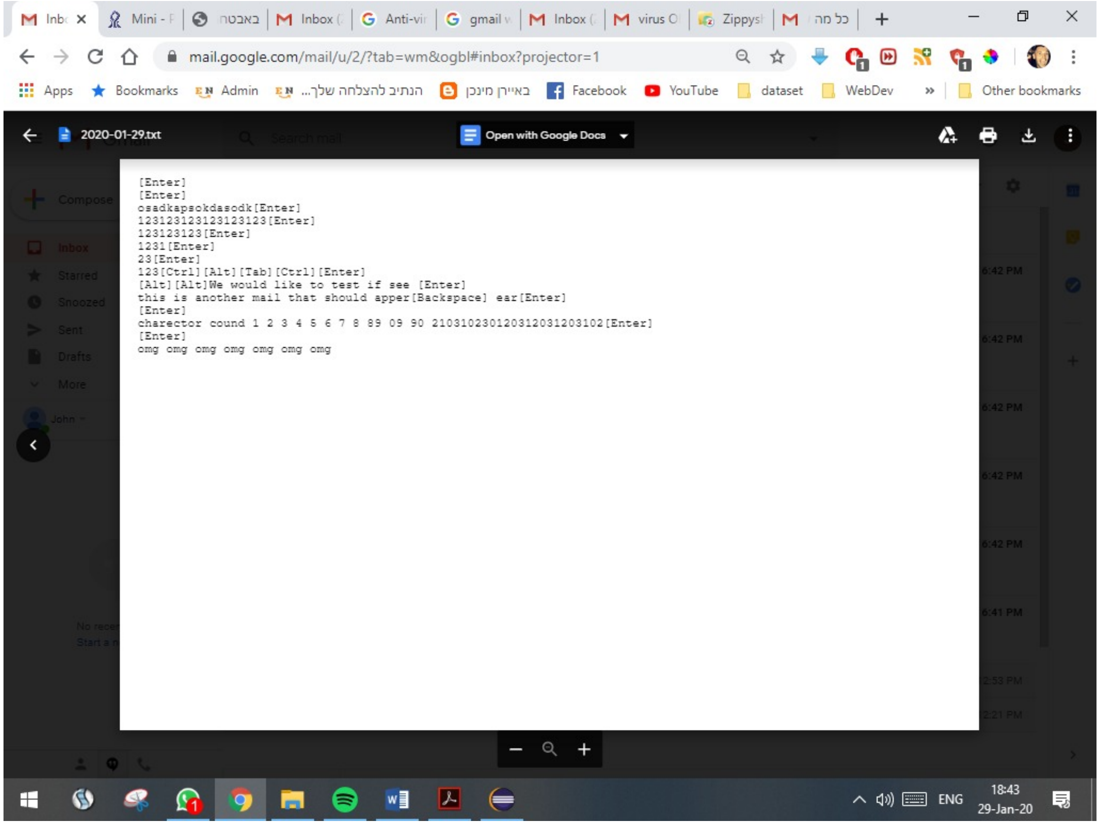
me (s)AINT - if see [Enter] this is another mail 6:42 PM
2020-01-29 18-... 2020-01-29.txt

me (s)AINT - [Ctrl][Alt][Tab][Ctrl][Enter] [Alt][Alt]We would like to test 6:41 PM
2020-01-29 18-... 2020-01-29.txt

Google 2 Critical security alert - Access for less secure apps setting has been turned on ourjank... 12:53 PM

Google Community Te. Finish setting up your new Google Account - Google banner Hi John, Welcome to Googl... 12:21 PM

Figure 5: Gmail interface with the new messages (notice that the time matches!)



```
[Enter]
[Enter]
osadkapsokdasodk[Enter]
123123123123123123[Enter]
123123123[Enter]
1231[Enter]
23[Enter]
123[Ctrl][Alt][Tab][Ctrl][Enter]
[Alt][Alt]We would like to test if see [Enter]
this is another mail that should apper[Backspace] ear[Enter]
[Enter]
charector cound 1 2 3 4 5 6 7 8 89 09 90 2103102301203120312031 02[Enter]
[Enter]
omg omg omg omg omg omg omg
```

Figure 6: additional view from inside the file

6 References

- What is a Keylogger? https://combofix.org/what-is-a-keylogger-virus-and-how-to-remove-it.php
- jNativeHook API https://github.com/kwhat/jnativehook
- Apache mail API https://commons.apache.org/proper/commons-email/
- Keylogger instructions and implemintaion https://github.com/tiagorlampert/sAINT