**Exploiting Windows Startup Feature Using Batch File and Python Script**

A PROJECT REPORT

**Under the guidance Of**

**Mr.G.Munisai,**

**Submitted by**

**Viswa Teja Vengala (180201029)**

**P Deepak Kumar (180201023)**

**TC Rayudu Babu (180201027)**

**D Srilatha (180201005)**

in partial fulfillment of the academic

Requirements for the award of

**Post Graduate Programme**

**IN**

**Cyber Security**

International Inistitute Of Digital Technologies

IIDT Office, Airport Road, Renigunta, Tirupati,

Andhra Pradesh, India- 517520,

E-mail: info@iidt.edu.in, Tel : 0877-2275770/72/73

.

**CERTIFICATE**

This is to certify that the project report entitled “**Exploiting Windows Startup Feature Using Batch File and Python Script**” being submitted by **Viswa Teja Vengala (180201029), P Deepak Kumar (180201023), TC Rayudu Babu (180201027),**

**D Srilatha (180201005)** in the partial fulfillment of the requirement for the award of the degree of **Post Graduate Programme In Cyber Security** from **IIDT** is a record of bonafide work carried by them during the academic year 2018-2019.

**Mr.G.Munisai Mr.B.Krushna Chaitanya**

Internal Guide Head of the Department

External Examiner

International Inistitute Of Digital Technologies

IIDT Office, Airport Road, Renigunta, Tirupati,

Andhra Pradesh, India- 517520,

E-mail: info@iidt.edu.in, Tel : 0877-2275770/72/73.

**DEPARTMENT OF CYBER SECURITY**

**DECLARATION**

We, **Viswa Teja Vangala(180201029), P Deepak Kumar (180201023), TC Rayudu Babu (180201027), D Srilatha (180201005)** hereby declare that the project entitled **“Exploiting Windows Startup Feature Using Batch File and Python Script”** is being submitted by us in the partial fulfillment of the requirement for the award of the degree of **Post Graduate Programme In Cyber Security** from **IIDT** and is a record of bonafide work carried out by us under the guidance of **Mr.B.Krushna Chaitanya, Head Of the department, Cyber Security**.

**Viswa Teja Vengala (180201029)**

**P Deepak Kumar (180201023)**

**TC Rayudu Babu (180201027)**

**D Srilatha (180201005)**

**ACKNOWLEDGEMENT**

We take this opportunity to express our deepest gratitude and appreciation to all those who have helped us directly or indirectly towards the successful completion of this mini project.

We owe our thanks to **Mr.G.Muni Sai, Internal Guide**, for his immense support and giving necessary guidance.

We express our gratitude to **Mr. B.Krushna Chaitanya, Head of the Department,** for his constant co-operation ,support and for providing facilities throughout the **Post Graduate Programme In Cyber Security** .

We express our gratitude to all the faculty of our Department for their co-operation and keen interest throughout this mini project.

**Viswa Teja Vengala (180201029)**

**P Deepak Kumar (180201023)**

**TC Rayudu Babu (180201027)**

**D Srilatha (180201005)**

**Examiner's Certificate**

This is to certify that the project report of **Viswa Teja Vengala** Reg.No **180201029, P Deepak Kumar** Reg.No **180201023, TC Rayudu Babu** Reg.No **180201027, D Srilatha** Reg.No **180201005**  entitled **“Exploiting Windows Startup Feature Using Batch File and Python Script”** is approved and is acceptable in quality and form.

Internal Examiner External Examiner

**CONTENTS**

**Chapter Page.No**

1. **Abstract 00**
2. **Introduction 00**
3. **Hardware Requirements 00**
4. **Software Requirements 00**
5. **Feasibility Study 00**
6. **Screen Shots 00**
7. **Conclusion 00**

**ABSTRACT:**

Windows operating system is very user friendly and advance which is used by millions of people around the world. Sometimes few features can be used to exploit the user. We found a way to execute any script automatically which contains code that can exceed memory and CPU utilization and causes system to not respond. Even we can execute commands and retrieve system data from the victim. The malicious script is executed every time while system start up with the help of a simple windows batch file placed in startup folder.

**INTRODUCTION:**

The startup folder is a feature available in Windows operating systems that enables a user to automatically run a specified set of programs when Windows starts. The startup folder was introduced in Windows 95. It contains a list of applications or programs that run automatically whenever the computer boots up. It is usually located in the programs folder that can be opened by clicking the start button. The location of the startup folder may vary slightly in different versions of Windows. Any program that needs to be run automatically on boot-up must be stored as a shortcut in this folder. The startup folder is a feature that is included in Windows to provide convenience for its users. It allows users to gain instant access to the programs they frequently use. The shortcuts stored in this folder open automatically every time the computer boots. Items in the startup folder can include any type of executable application such as a word processing application, mail client, Web browser or even a particular file or document that the user may want to open whenever they start their system. Individual files can be added to the startup folder in the same way as applications by creating a shortcut and placing it in the startup folder.

The batch file is a term which often falls on the ears of Windows users. Basically, it’s a way of doing things without actually doing them. You might be aware of the Windows command line interpreter known as CMD or Command Prompt. It takes various commands as input through the keyboard and processes them. Being a Windows user, most of us aren’t much comfortable with anything that doesn’t look good, and CMD is one of them. A batch file does the work of a mediator between you and the command prompt. It is a file – with .bat, .cmd,. btm file extensions – containing the CMD commands. When you run a batch file, the commands written in it are executed in the Command Prompt following a serial fashion. Otherwise, these would have to be entered manually line by line. A batch file saves your time, otherwise, would be invested in typing the same commands again and again.

**FEASIBILITY STUDY:**

A simple python script can be used to create games to automate tasks and even perform various attacks on the system. A python can be used to generate a executable file which contains script to execute windows commands. These commands can be fetched from a remote server where the attacker stores the commands. Using network packages and cmd command execution package available in python we can get the commands from the remote server and execute those commands.

1. **Economical Feasibility:** It is economically feasible as it requires only python tools to develop and a free hosting server to run commands remotely. Unlike Metasploit, attacker can execute commands from anywhere and anytime
2. **Technical Feasibility:** This study is carried out to check the technical feasibility, that is, the technical requirements of the system. The system may have basic technical requirements such as python development kit, IDE and internet connection.
3. **Social Feasibility:** The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it.

**SYSTEM REQUIREMENTS:**

1. Windows 10 Operating system
2. Intel i3 clocked at 1.6GHz
3. RAM 4GB
4. Hard disk 100GB
5. python IDE
6. Internet connectivity

**SCREENSHOTS:**

Attacker must send the pong\_game.exe malicious file to the victim.

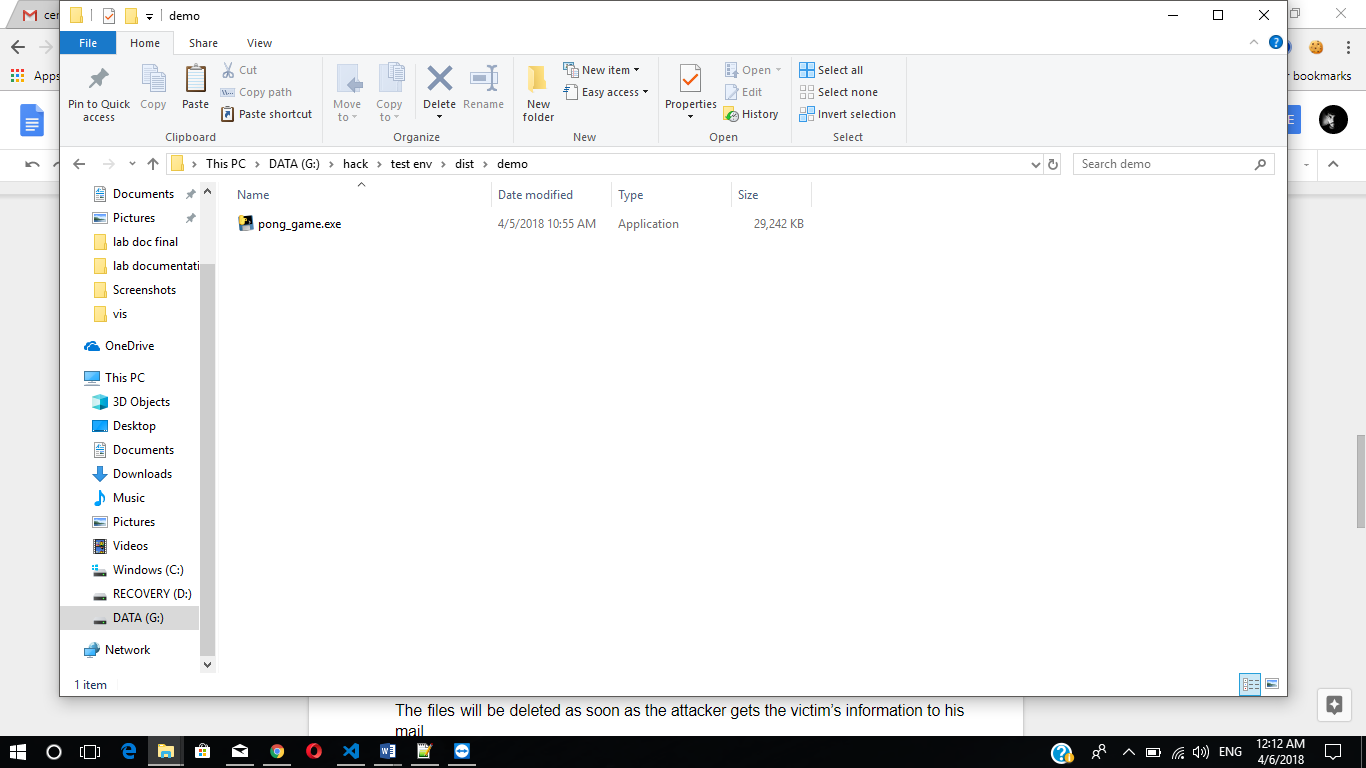


Fig 1. Pong game file

When the victim runs the game, the following steps are performed

1. The game starts downloading malicious backdoor program gameData.exe from the server and place in some known location.
2. A bat script is generated with contain command to run gameData.exe
3. A shortcut file is generated for the batch file and moved to startup folder.

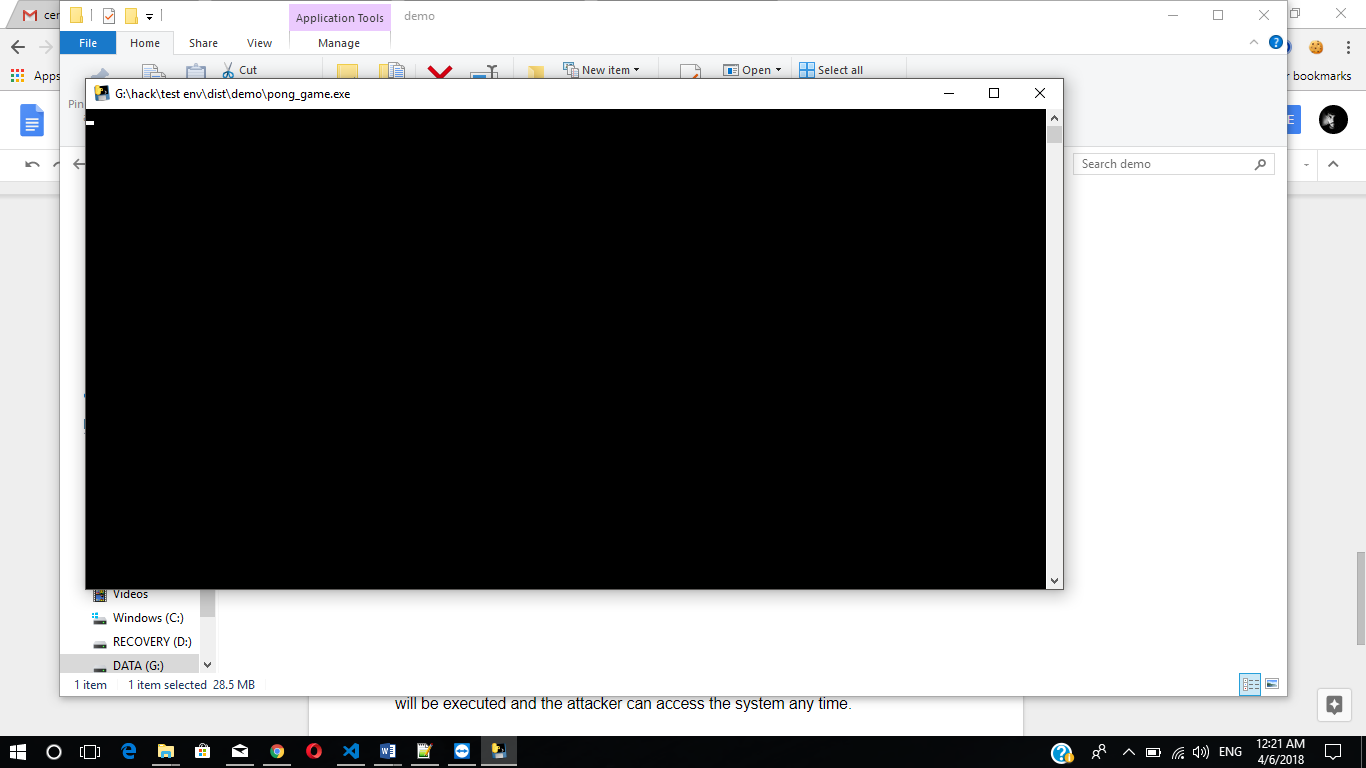


Fig 2. Pong game downloading the malicious backdoor file

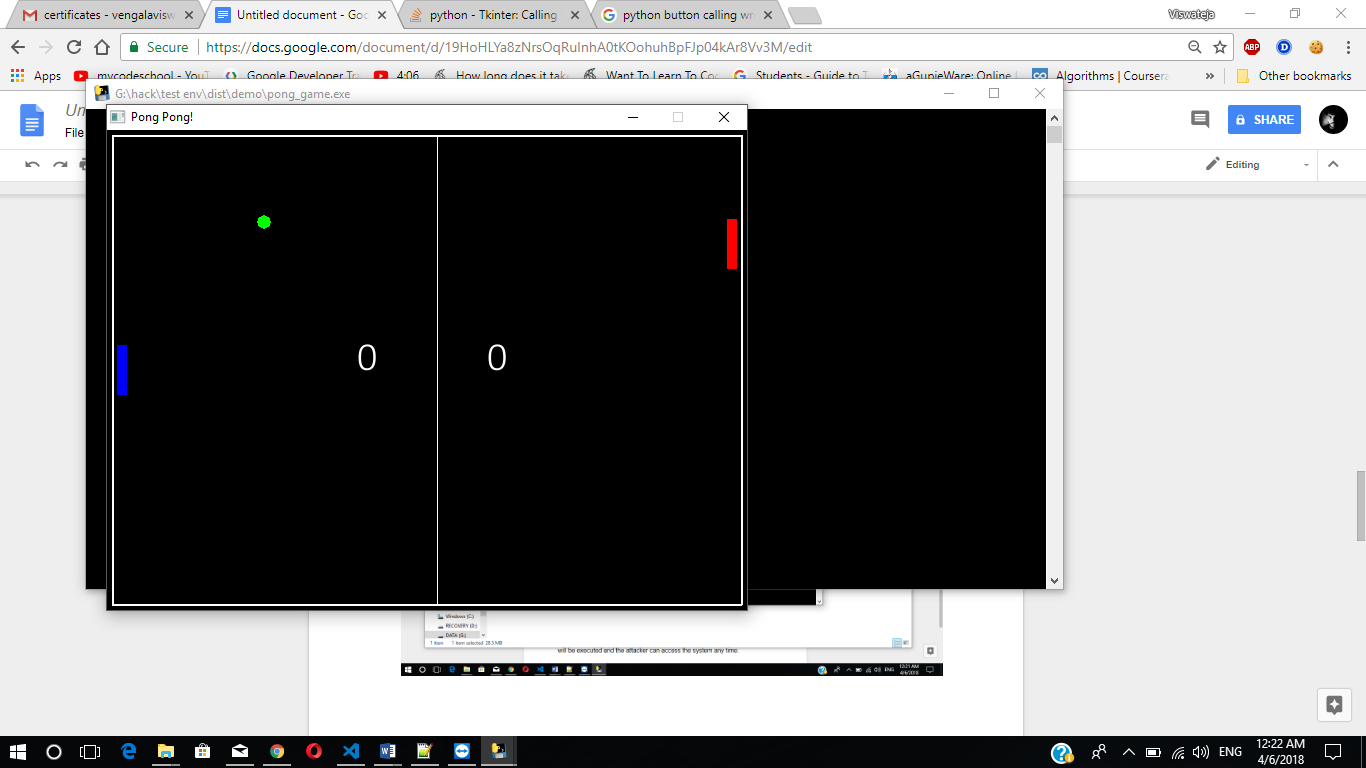


Fig 3. Pong game execution

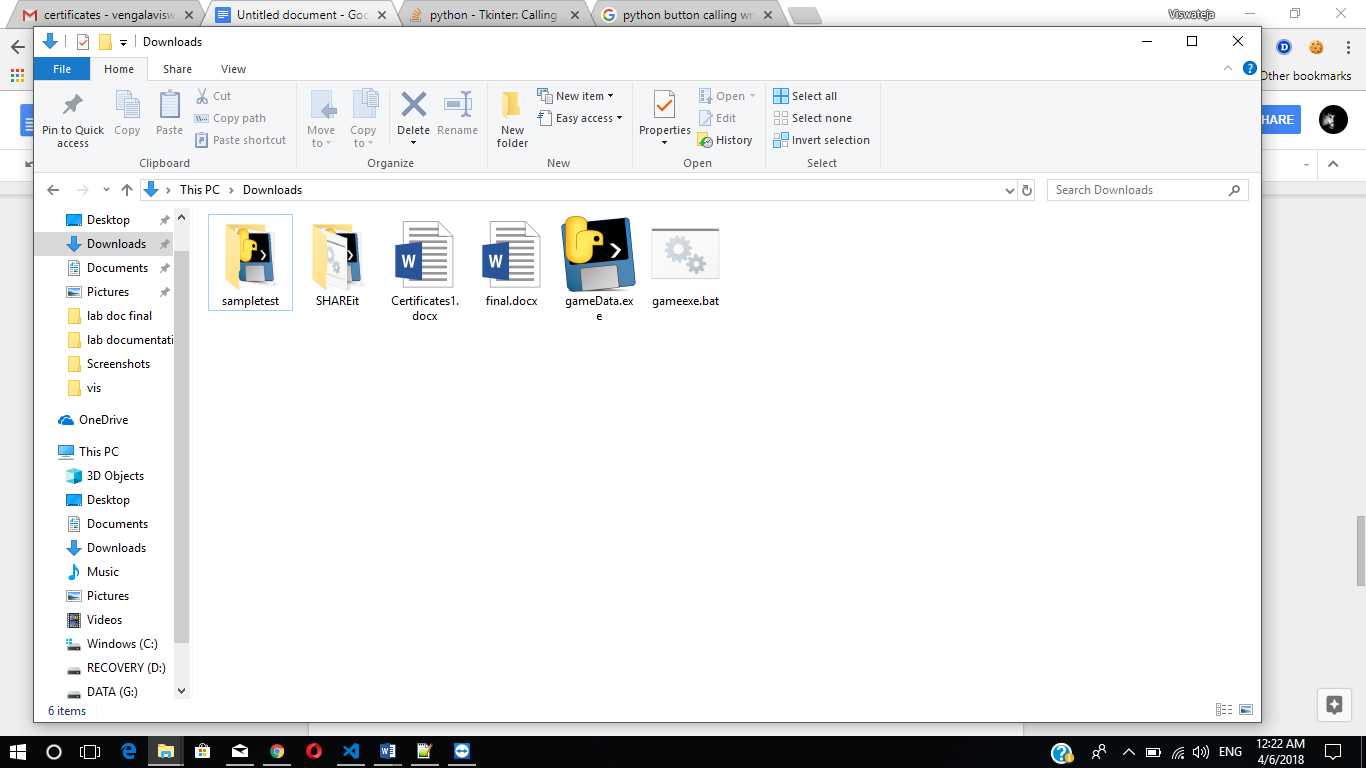


Fig 4. gameData.exe backdoor and gameexe.bat files generated

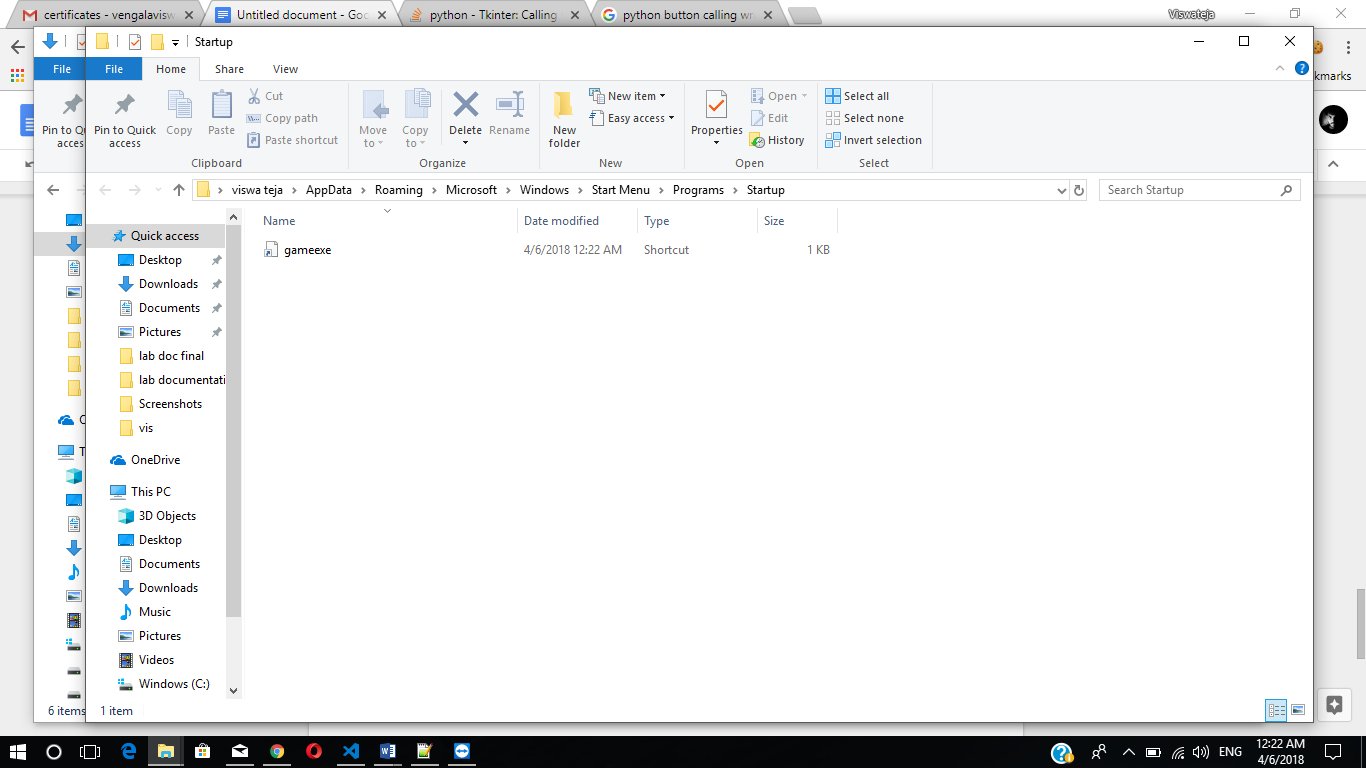


Fig 5. Gamexe.bat file shortcut file placed in startup folder

Now, every time the victim starts the computer, the bat file present in the startup folder executes the gameData.exe. The gameData.exe gets the known wi-fi names and passwords and send a mail to the attacker and executes remote command saved in the text file hosted in a remote server. The gameData.exe runs as a hidden process and keep on executing the commands till “exit loop” command is entered.

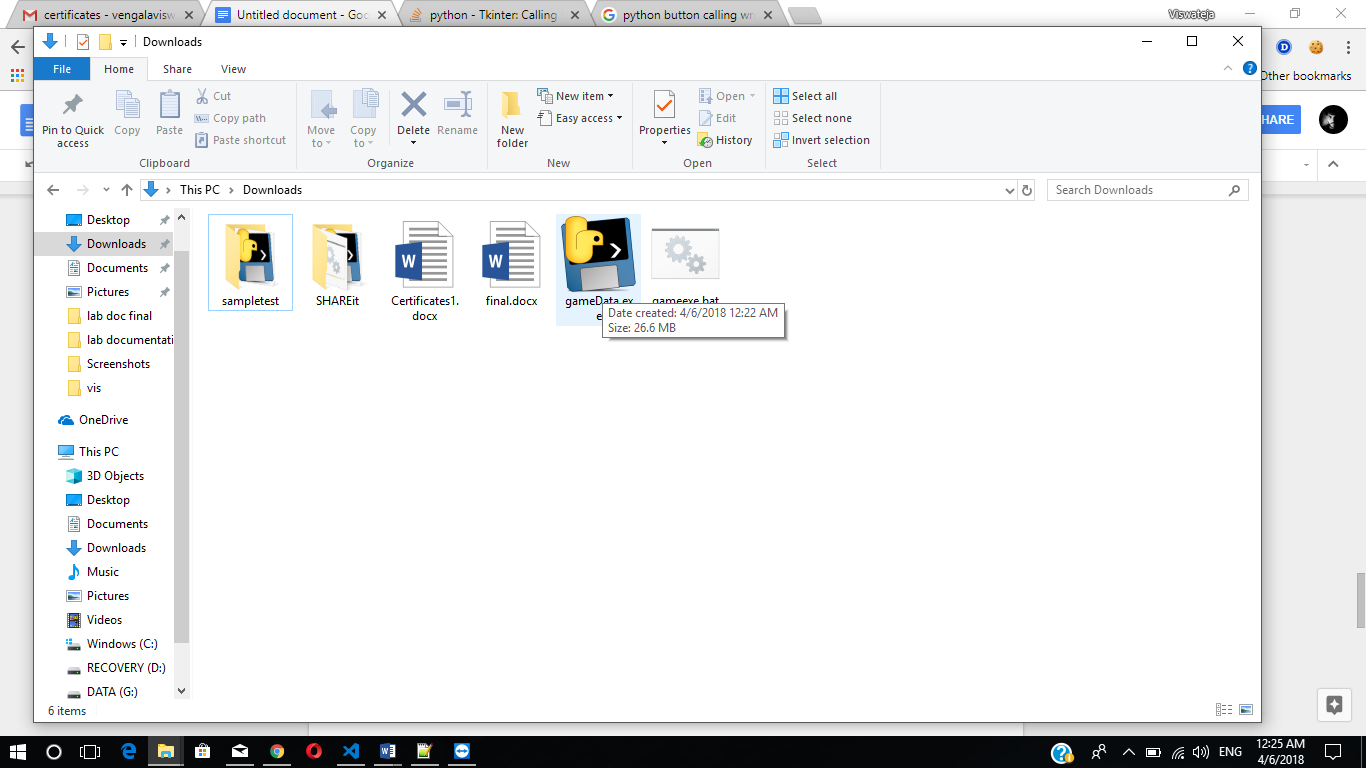


Fig 6. gameData.exe is executed by the batch file

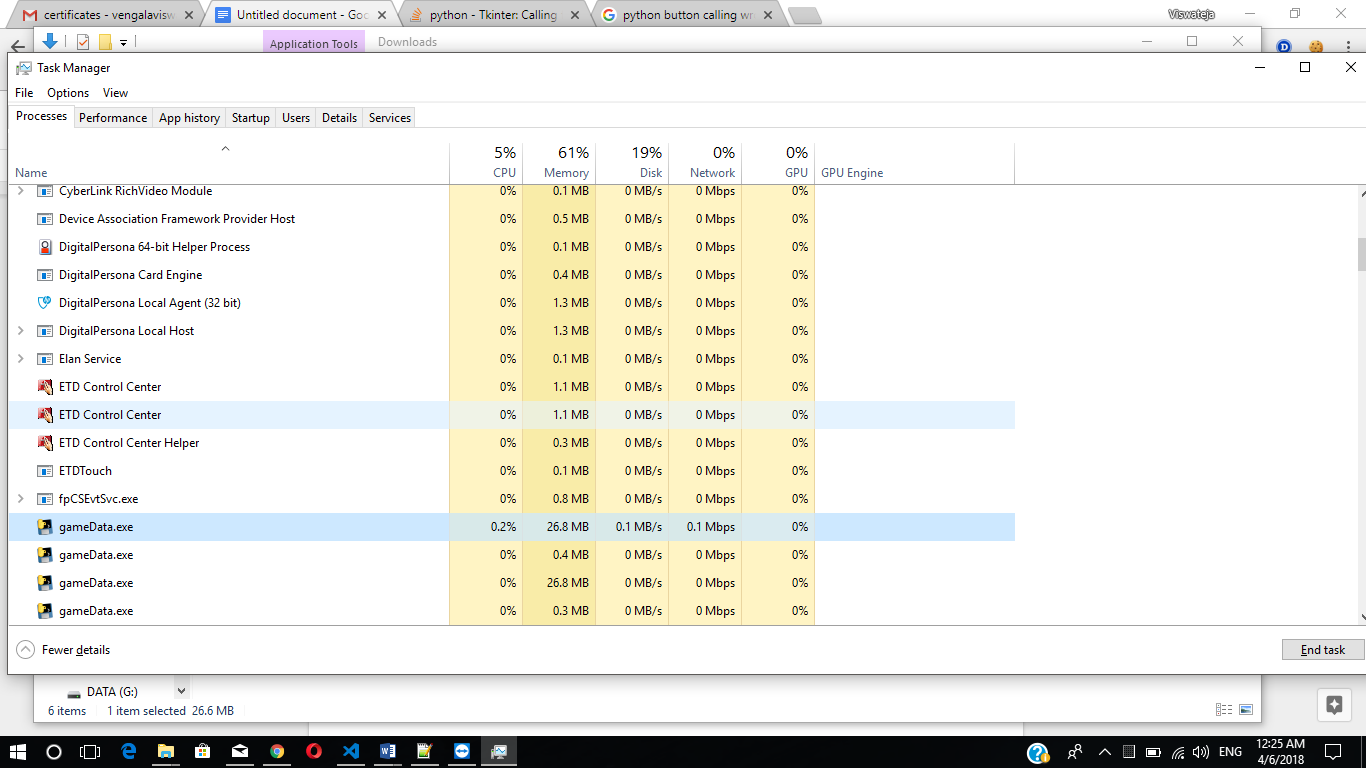


Fig 7. gameData.exe running as hidden process

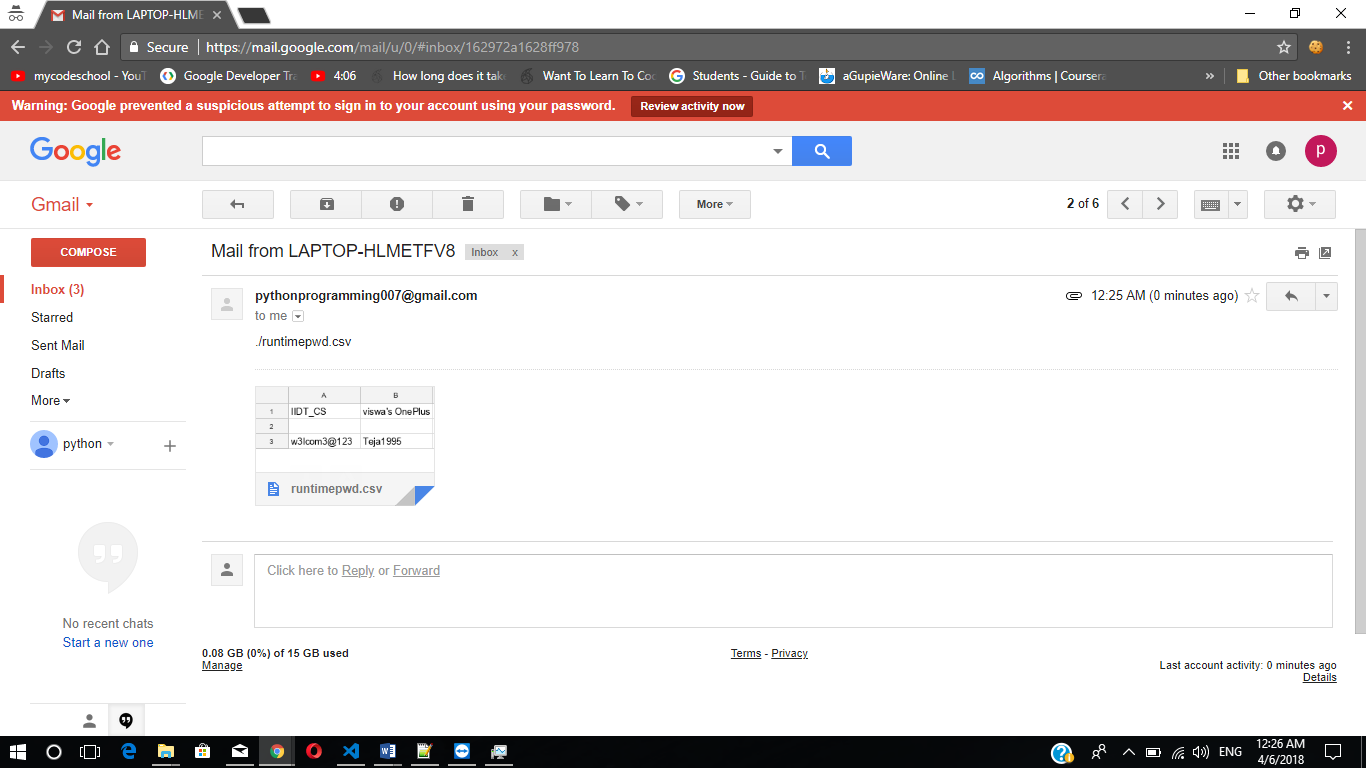


Fig 8. Details of wi-fi names and passwords mailed

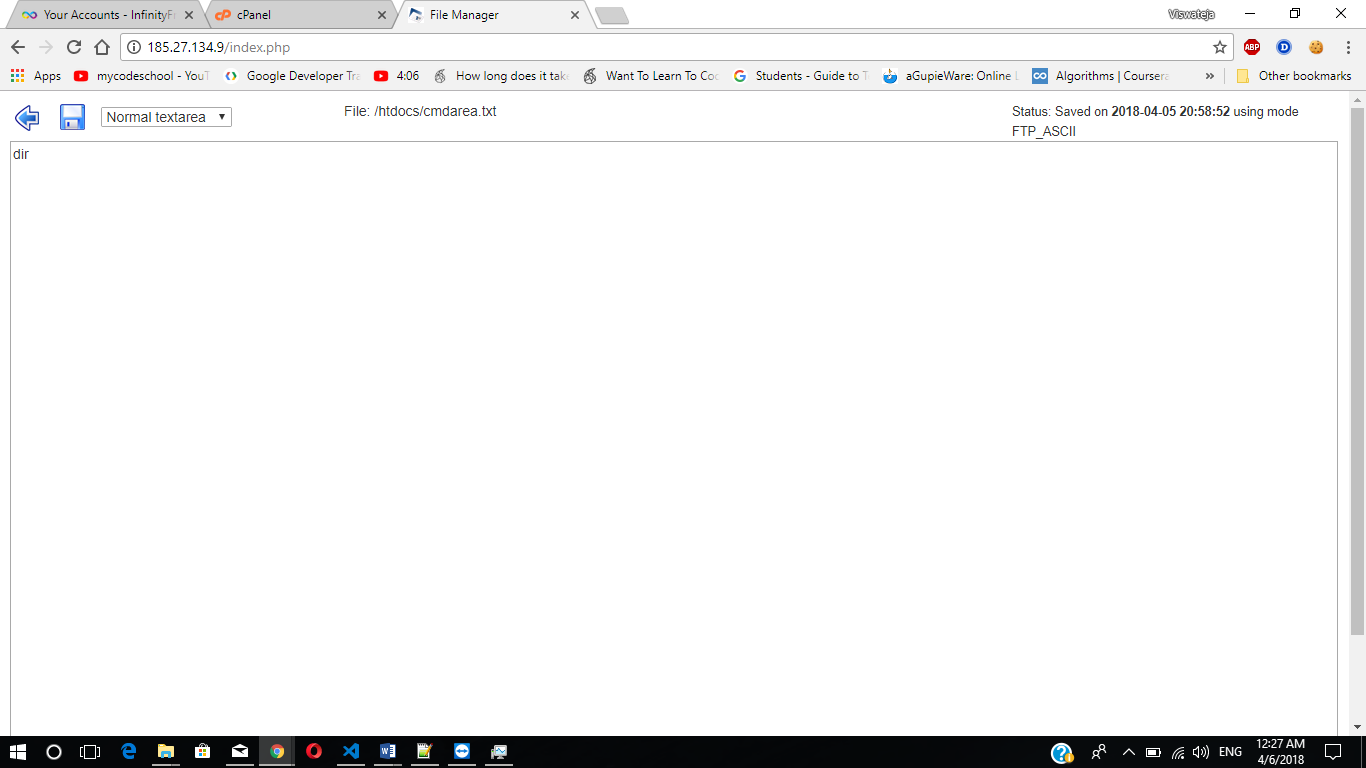


Fig 9. Remote text file to store commands

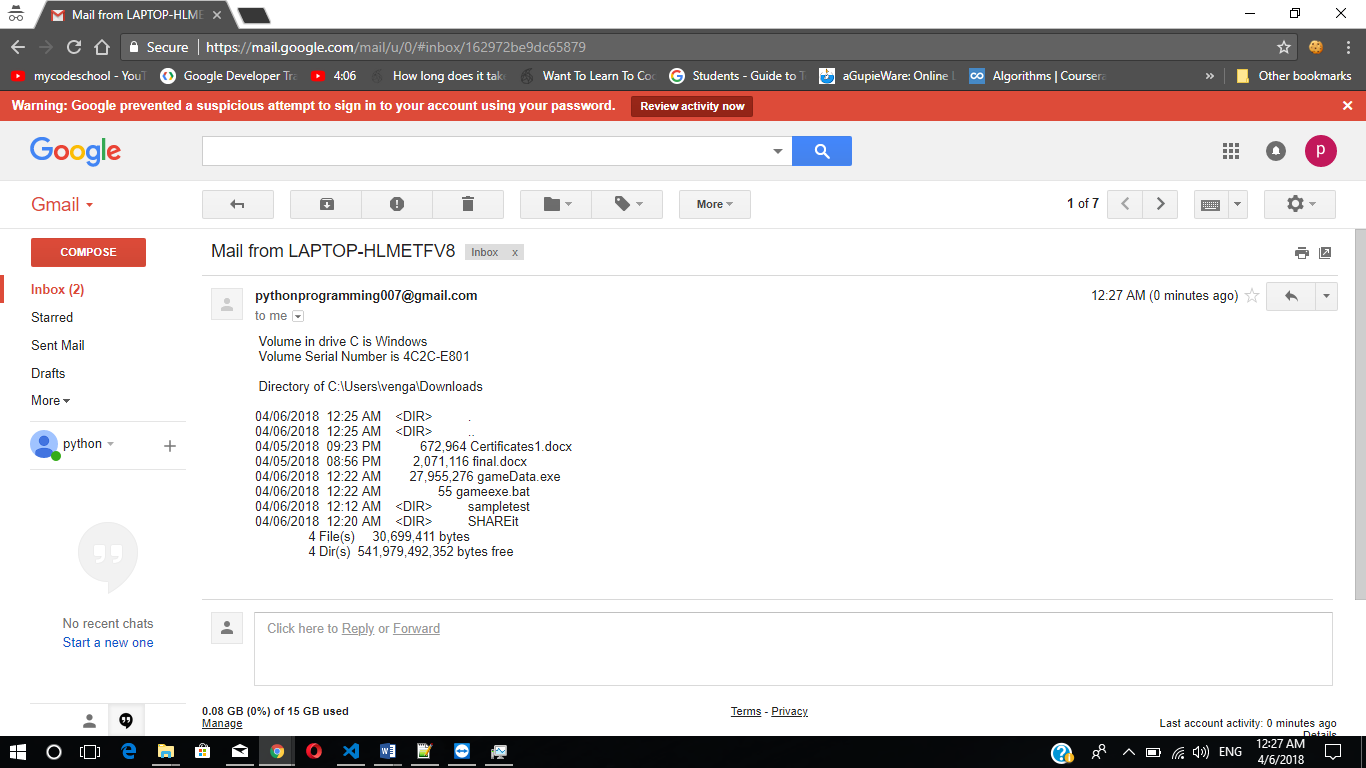


Fig 10. Response of command executed mailed

**CONCLUSION:**

Simple batch file and python script can be used to AutoStart a program and use it as backdoor to gain or harm a system