International Journal of Scientific Research in Science, Engineering and Technology
Print ISSN: 2395-1990 | Online ISSN : 2394-4099 (www.ijsrset.com)
doi : https://doi.org/10.32628/IJSRSET

Backdoor Based Attacks

Dr. Sunil Bhutada[1], A. Lokesh[2], S. Ashok Reddy[2], M. Narasimha[2]

[1]Professor, IT Department Sreenidhi Institute of Science and Technology Yamnampet, Hyderabad, India

[2]B. Tech, IT Department Sreenidhi Institute of Science and Technology Yamnampet, Hyderabad, India

Article Info
Volume 9, Issue 3

Page Number : 418-423

Publication Issue :
May-June-2022

Article History
Accepted : 01 June 2022
Published: 10 June 2022

ABSTRACT

Hacking is a method to exploit the vulnerabilities of a computer system and to gain access, information, privacy invasion, etc., costing many companies a huge amount of money and resources. Through python where it is a high-level programming language, and is also used in hacking as it is supported on all operating systems and many libraries related to cybersecurity. Among many techniques and tools used in hacking, the back door is a most common and useful way of attacking a computer or network. Its main purpose is to send and receive data, mostly commands, through a port to another system. Basically, the hacker installs a malicious program on the victim's computer, which executes (on the victim's computer) all the commands given by the hacker. To build our locally-working backdoor, we will use the socket module. Sockets and the socket API are used to send messages over the network. As we already know to send messages, there's who sends the message, here the Hacker, and who receives the message and replies, here the Victim. After the Victim runs the malware we'll create, it's going to set up this type of connection between the hacker's and victim's system. The backdoor attack is powerful because it can't always be detected; an antivirus can't stop you from installing an innocent-looking app.

Keywords - Socket, port, TCP connection, Backdoor, Virtual Machine, base64 encoding and decoding.

I. INTRODUCTION

Protecting one's data in this era where it is purely dominated by machines and systems which could be running autonomously or supervised by others has been a tough task. Where people are trying their best to protect the data while others are trying to gain access to the system or data through various ways like using Brute Force, being an inside job, or secretly hacking a system without the knowledge of the User which could cause a data breach and it costs many companies millions of dollars. The Backdoor is a simple program that when executed in the victim's system gives the remote access to the Hacker over the victim's system without their knowledge and permissions by initiating a connection to the attackers system with the help of Sockets. This malware (backdoor) will be installed and executed into the victims system on its own without the user initiating it. Once it is executed it runs in the background waiting for the attacker's commands to exploit the user system. The main purpose of this backdoor is to gain access over the

Copyright: © the author(s), publisher and licensee Technoscience Academy. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited

victims system and to manipulate the data stored in the victim's system. The data (text files, jpg, jpeg, etc.,) could be downloaded from the host (victims system), manipulate the downloaded files, and upload from the attackers system to the host system. If the attacker really wanted to take down the host system they could upload viruses and destroy the system from inside. No matter how secure the user system is, once the user tries to download a wrong file or program consisting of a malicious program their system gets compromised. This malware could even be hiding in your mostly used software or other applications like anti-virus software and other apps installed in your system. This malware is mostly in the networking system to initiate many firewalls that fail to detect the malicious malware because they look similar to the usual traffic they see in the web page or web server interactions. The simple way to avoid such malware is to just not trust all applications and software, and don't accept the terms and regulations of various applications without knowing what they state or the software they require to install and run. Download software or an application if and only if you trust it.

II. OBJECTIVE OF PROJECT

The main objective of our project is to let the users know about the method called as Backdoor which is mainly and most commonly used by an Attacker to gain access and control over a user's system by creating a connection between the systems using sockets, it runs in the background and terminates the connection when the users system is shut down and restarts again once the system is turned on automatically without the user initializing the malware. Our objective is to show how the attackers use a few lines of code to gain access to the users system and how to avoid downloading suck malware.

III. SCOPE OF PROJECT

The main objective of our project is to let the users know about the method called as Backdoor which is mainly and most commonly used by an Attacker to gain access and control over a user's system by creating a connection between the systems using sockets, it runs in the background and terminates the connection when the users system is shut down and restarts again once the system is turned on automatically without the user initializing the malware. Our objective is to show how the attackers use a few lines of code to gain access to the users system and how to avoid downloading suck malware.

IV. SYSTEM DESIGN

The main objective of our project is to let the users know about the method called Backdoor which is mainly and most commonly used by an Attacker to gain access and control over a user's system by creating a connection between the systems using sockets, it runs in the background and terminates the connection when the user's system is shut down and restarts again once the system is turned on automatically without the user initializing the malware. Our objective is to show how the attackers use a few lines of code to gain access to the user's system and how to avoid downloading suck malware.

2.1. KEYLOGGERS:

Keyloggers are malicious software/spyware where the program records the keys pressed on the physical keyboard during a session and sends a report to the instructed email for every given time period until the keylogger stops, that is whenever the host system is turned off the malware also turns off and restarts by itself when the host system is turned back ON. But the malware doesn't recognize the keys pressed by the user they use a virtual keyboard on the system screen, The

developer still gets the report but it would be null unless they press a key on the physical keyboard. These Keyloggers can be detected and avoided by proper Anti-Virus software

2.2. Common Features:

- Stores Activity logs locally (Local Keyloggers).
- Report Activity logs to email (or) remote server
- Start with system start up.
- Re-establishes the connection once the host system turns back ON.

2.3. Application of Keylogger:

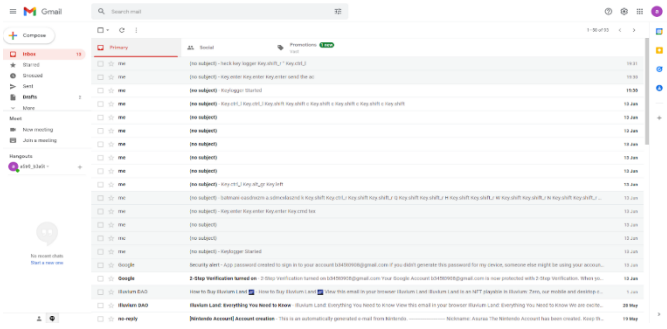
Generally, this kind of software is mainly used by software companies to keep their employees in check and observe their work for a certain time period. These are generally used to take an activity log of their employee's work for a particular amount of time interval, and send the report through the means specified by the developer. This prevents the employees to misuse the office systems for their personal gain or use. This makes them focus on their work and prevents them from any distractions. These are also used to spy on a user and to also gain critical information over users' passwords, user IDs, credit card information, and other personal information. These are unethical ways of using the Keyloggers. But there can be easily detected. Since a lot of time has passed the technologies have evolved and keyloggers have also evolved with time, they have been upgraded to better technologies where the companies keep a track of the activity log of their employee (work systems only) which will be stored in their server.

2.4. REPORT FUNCTION:

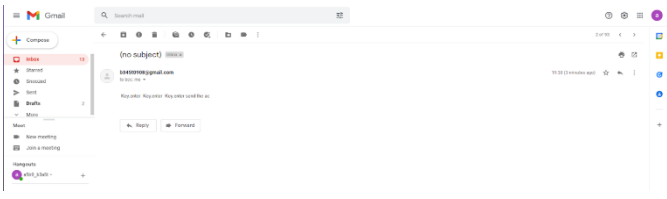
This Function Helps the user in Reporting the Activity log through the specified medium and to the specified destination as per the given instructions. The report Function helps in collecting the data of the Activity log which will be temporarily stored in the given space where parallelly it continues to record the Activity Log, when the given time interval comes it sends the collected Activity Log to the destination depending on the type of the Key-Logger like Remote Keylogger, Hardware-based Keylogger, Local Keylogger. Depending upon the type of the Keylogger there will be a destination address where the stored Activity log will be sent. There are three major functions to the Report Function, they are as follows:

- Runs in Background
- Doesn't Interrupts the program execution
- Every X(Time Interval) seconds, sends the report to the destination.

2.5. RESULTS:



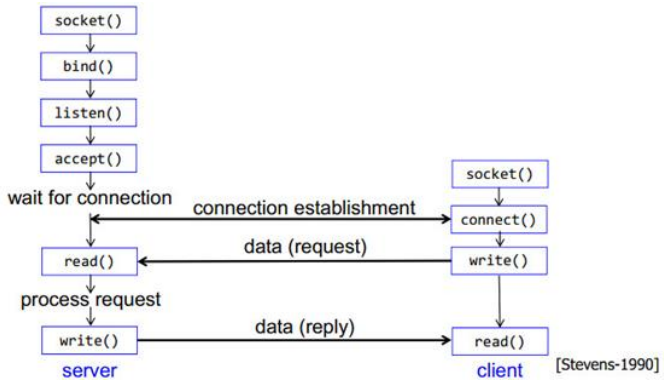
Activity report in the mail



Activity logs in the given time interval

3.1. BACKDOOR ATTACK:

The model was built using the methods. As shown below, the model defines the various steps of implementing our project.



3.2. IMPLEMENTATION

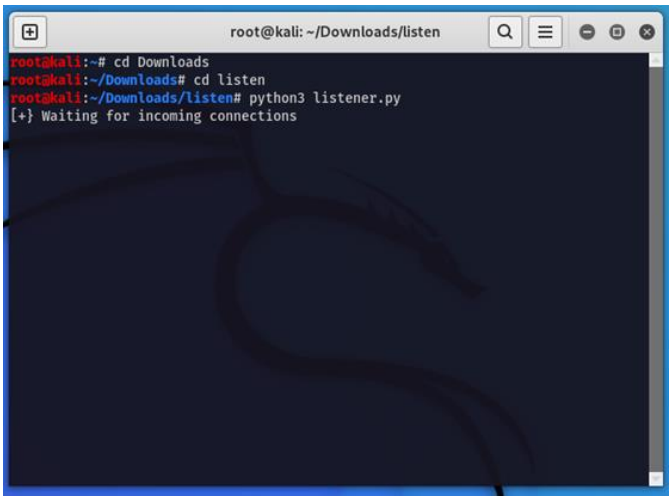
For this project, we used Python Programming Language to write the code.. Python provides a wide variety of libraries for scientific and computational usage. Libraries used for Reverse Backdoor are socket, JSON, Shlex, Base64, and libraries used for listeners are shutil, sys, Base64, OS, JSON, Socket, and Subprocess. The main functionalities used in the project are

1. Phishing:
   Sending the malware executable file through any social media as bait.
2. Executable Malware File:
   Whenever the victim clicks the file, it gets downloaded into the victim's local directory.
3. Malware Execution:
   As soon as the file gets downloaded, the malware executes itself without user interference on the port.
4. Connection Establishment:
   The connection will be established to the hacker's control panel (Linux command prompt/Terminal).
5. Manipulation of Victim's Data:
   The Victim's data can be manipulated by the hacker through the connection which was previously established.

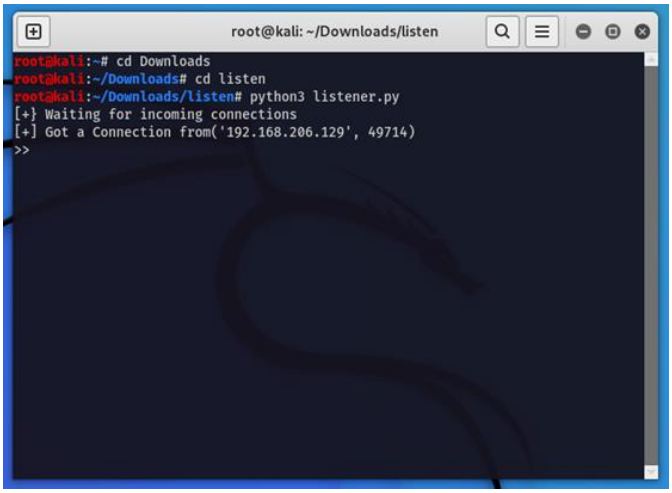
- Upload New Data into the Victim's System.
- Change the existing data.
- Change the file privileges
- Download data from the victim's system.

3.3. RESULTS

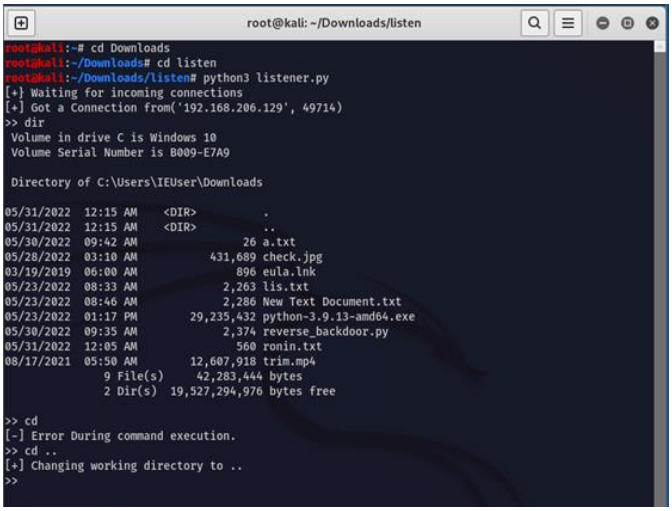
After the Execution of malware, the outputs of the above steps are shown as:



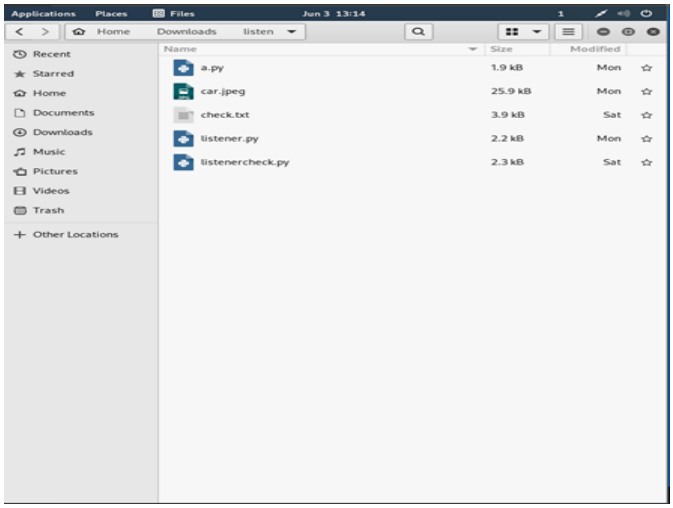
Waiting for malware to execute in the victim's system



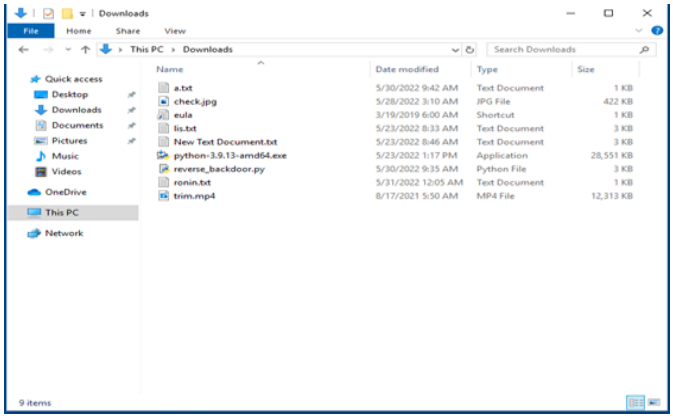
Connection from Victim's system successfully established



Navigating through the Directories in the victim's system



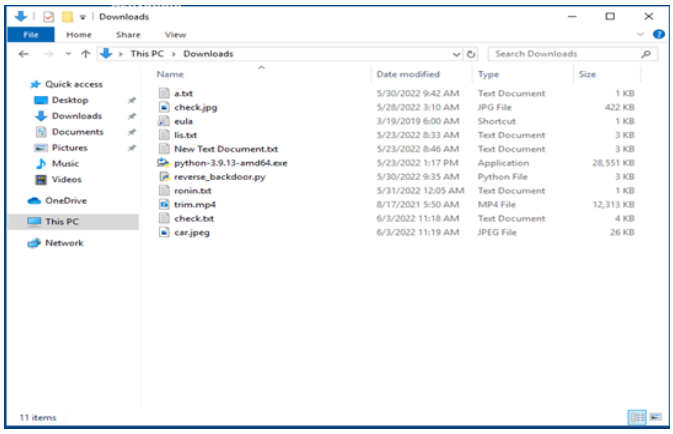
Existing files in Hackers' system



Existing files in Victim's System

```
>> upload check.txt
[+] Upload successfull.
>> upload car.jpeg
[+] Upload successfull.
>>
```

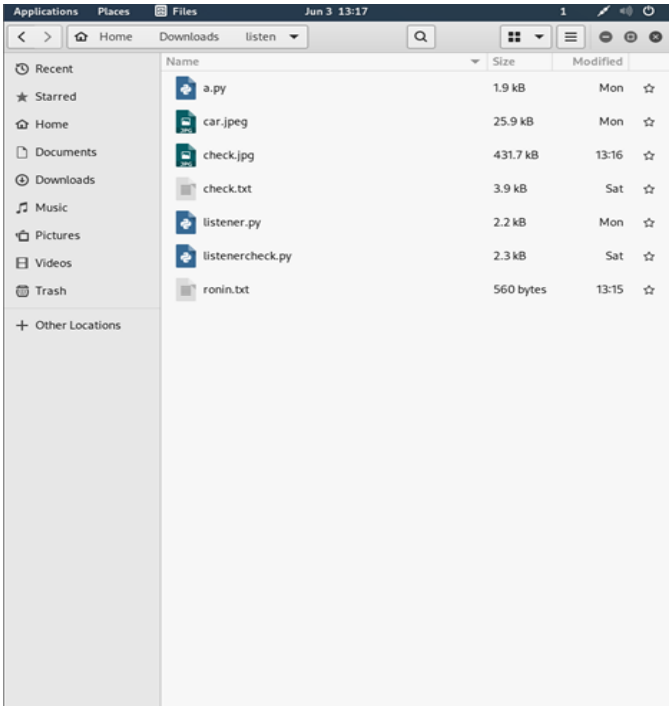
Successful upload required files from hacker system to victim system



Files in Victim's system after upload

```
>> download ronin.txt
[+] Download Successful
>> download check.jpg
[+] Download Successful
>>
```

Successful download of required files from victim's system to hacker's system.



Files in hacker's system after successful Download.

V. CONCLUSION

A backdoor allows the attacker to work with an infected computer as if it was his/her own PC and use it for various malicious purposes or even criminal activities. In most cases, it is really hard to find out who is controlling the parasite. In fact, all infections of such type are very difficult to detect.

They can violate user privacy for months and even years until the user will notice them. The malware author can use it to find out everything about the user, obtain and disclose sensitive information like passwords, login names, credit card numbers, exact bank account details, valuable personal documents,

contacts, interests, web browsing habits, and much more.

Furthermore, these parasites can be used for destructive purposes. If the hacker cannot obtain any valuable and useful information from an infected computer or has already stolen it, he/she eventually may destroy the entire system to wipe out digital footprints. This means that all hard disks would be formatted, and all the files on them would be fully erased.

VI. REFERENCES

[1]. Backdoor - https://www.tutorialspoint.com/what-is-a-backdoor

[2]. Socket - https://docs.python.org/2/library/socket.html

[3]. Json - https://docs.python.org/2/library/json.html

[4]. Python Networking Programming - https://www.tutorialspoint.com/python/python_networking.htm

[5]. https://www.2-spyware.com/backdoors-removal - How to Avoid Backdoor

[6]. Smtplib- https://docs.python.org/3/library/smtplib.html

[7]. Pynput- https://pypi.org/project/pynput/

[8]. Threading - https://docs.python.org/3/library/threading.html

[9]. Keylogger- https://resources.infosecinstitute.com/topic/keyloggers-how-they-work-and-more/

[10]. Google accounts - https://support.google.com/accounts/answer/185833?hl=en

Cite this Article

Sunil Bhutada, Sanjay Kiran Chennoju, Anvesh Gali, Manikanta Reddy Makka, Likith Chintala, "Enhanced Parking System", International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET), Online ISSN : 2394-4099, Print ISSN : 2395-1990, Volume 9 Issue 3, pp. 382-385, May-June 2022.

Journal URL : https://ijsrset.com/IJSRSET2293156