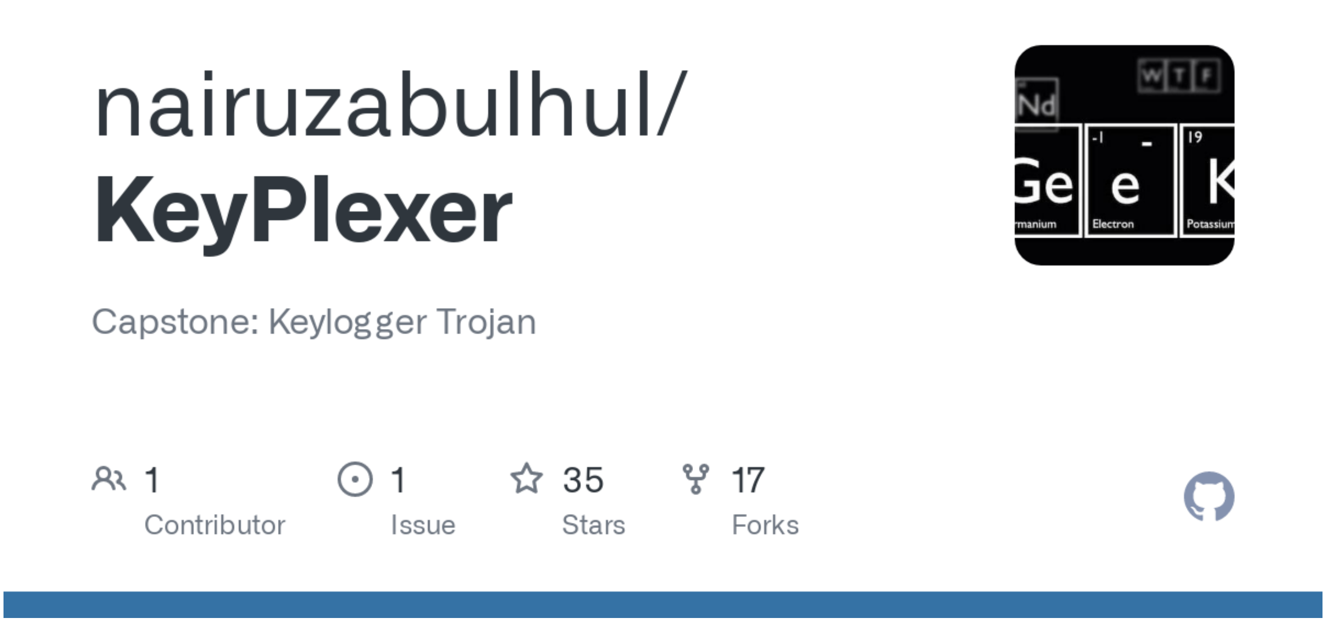
GitHub - nairuzabulhul/KeyPlexer: Capstone: Keylogger Trojan

github.com/nairuzabulhul/KeyPlexer

nairuzabulhul



nairuzabulhul/
KeyPlexer

Capstone: Keylogger Trojan

1 Contributor

1 Issue

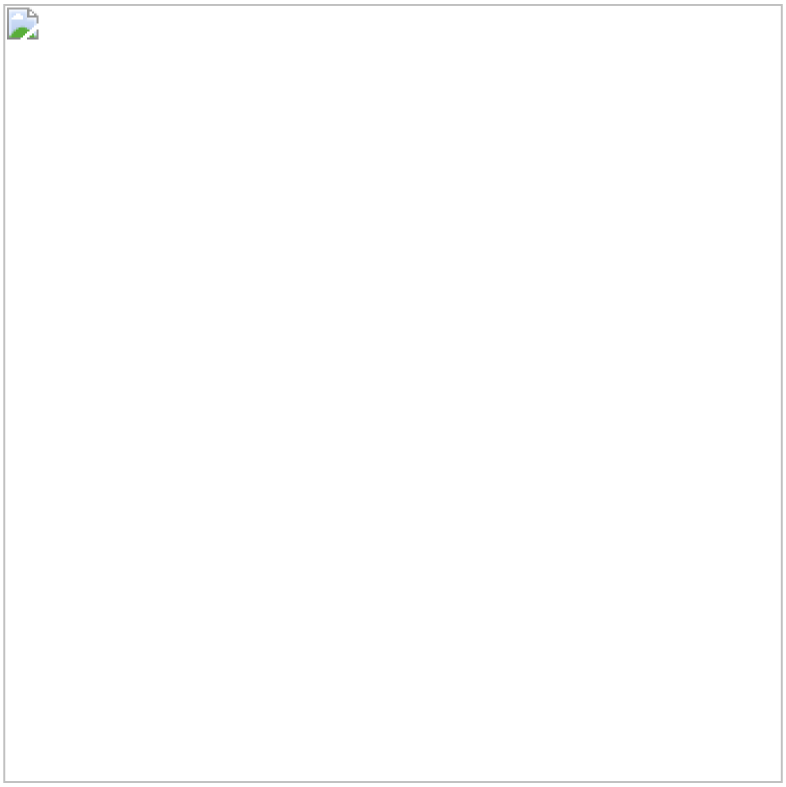
35 Stars

17 Forks

Project Description:

The project explores operating systems vulnerabilities in protecting against common threats of malware. The project will be a demonstration of how malware type Trojan is created and executed in the targeted machines.

Keyplexer is a Remote Access Trojan (RAT) written in Python. It combines the functionalities of Keylogger with remote access abilities. Meaning, that not only the program records all movements of the user, but also has access to the machine live through the created backdoor or Trojan.



Features:

[x] Logging ALL keystrokes of the user daily and save them in log.txt file

[ ] Keystrokes are sanitized for accurate output (Ctrl, Alt, Enter)

[x] Capture the clipboard contents

[ ] Detects when the user is accessing special important websites such as social media, banks, etc

[x] Capture ALL active windows on the host machine every 2 min

[x] Conceal and Hide the logs directory with its file on the victim machine

[x] Detects and saves all open programs in the machine with their paths

[x] Sends the logs over email at the end every 1h

[x] Permanently delete the log files after sending them over email to conceal traces

[x] Capture screenshots of the user machine and send them via email

[X] List all the running processors in the system

[ ] Interact with the processor (run it , or kill it)

[X] Files are renamed to unsuspicious names to avoid detection

[x] Checks the victim machine for internet connection, if the target computer is not connected to the internet, all logs and images will be saved locally and once connected it will start sending them all

[ ] Send email or text when the user shuts down the computer, logs off or disconnects from the internet

[ ] Added Persistence to the machine, to avoid disconnection on the restart

[x] Gets the Wifi credentials on the Accessed Point

[x] Get all the history of browsers (Chrome, Firefox)

[ ] Get al histrory, cookies, autofill, and saved password * [Histroy is DONE]

[x] Keplexer evades all signature based Anti-viruses

[x] Fingerprint the system and get all the information

[x] IP detection

[x] Revsershell is added as backdoor trojan

[X] Interactive shell -- move flexiblly around the user directories using cd command

[X] Download/ upload file using the backdoor shell functionality * [Download is DONE]

[X] DELETE images and logs after sending them through email using [cover] command

[X] Multiple Clients

[x] Trun the script into an executable

[X] Add colors to the server menu --linux

Additioal Steps:

[ ] Bind the program to a file with an icon

[ ] Encrypt traffic accross the network using AES encryption

[ ] Detect virtual environment

[ ] Webcam logging

[ ] Microphone logging

[ ] Get the system loging credentials

Nextstep

[ ] Send email or text when the user shuts down the computer, logs off or disconnects from the internet

[X] Added Persistence to the machine, to avoid disconnection on the restart

```
[X] Copy the file to another location and delete the current one
```

```
[X] Edit the registry
```

[ ] TESTING --> additional testing is required

[ ] Keystrokes are sanitized for accurate output (Ctrl, Alt, Enter)

[ ] Detects when the user is accessing special important websites such as social media, banks, etc

[ ] Interact with the processor (run it , or kill it)

Cleaning

[1] Persistence --> clean up the function

[2] Copy and hide the files in the system