­Project Report: Key Logger

By: Dan Sutter, Lauren Potersnak

**Objectives**

* + Create a keylogger
    - Records key typing of the victim
    - Screen captures the victim’s screens
    - Records what program the victim’s is using
    - Sends the key and screen captures to the attacker’s email
    - Runs undetected on an unprotected computer
  + Learn about how keyloggers work
    - How they are used maliciously
    - How they are placed on computers
    - How they can be protected against

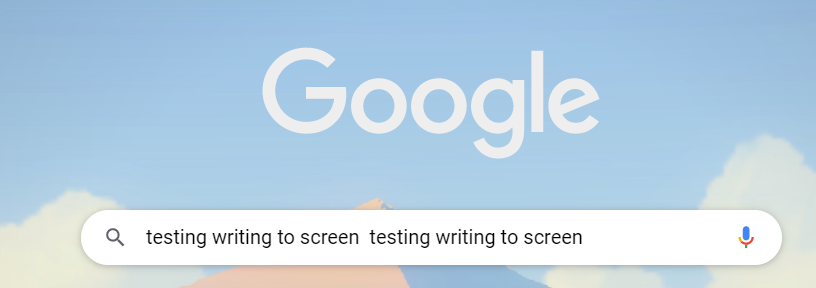
**High level design**

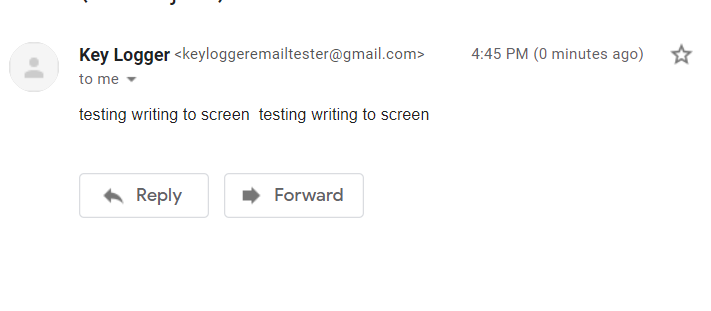
* + Key\_logger gets activated either by clicking on the pyw file or by attaching it to a trusted program with launch.bat
  + The Key\_logger.pyw runs in the background and periodically sends emails to the keylogger email
  + Keys logged with on\_press function and emailed with smtplib.SMTP\_SSL
  + Emails made readable by removing ‘’ and implementing a way to account for spaces and backspaces

**Implementation**

* + Implemented with python version 3.9 using pynput library functions
  + pyw to hide when the program is running on an unprotected computer
    - if the normal py used for the python program then a message of the program running will be shown to the victim
  + Our logger records the users’ keystrokes
    - works with on-screen keyboard
  + Our logger sends screenshots of the victim’s computer screen
  + The attacker obtains this information through email and the key logger periodically sends the information it has captured
  + Also Created a launch.bat file that can be attached to the victim’s internet explorer shortcut.
    - This would launch both the logger and internet explorer when the victim selects the internet explorer short cut

**Output**

* + Sample output of only text capture



* + Sample output of screen shot
    - //I think you said you had pics of this already so just add them here

**Challenges**

* + We could only test our logger with windows virtual keyboard, so we were not able to test its robustness against other virtual keyboards such as azerty or Dvorak.
  + Figuring out how to take screenshots with python was a bit of a challenge since we are both new to python. The screenshots that we were able to take only capture the main monitor so subsequent monitor readings would be missed making our keylogger less effective than we would like. The screenshots also do not get deleted from the victim’s computer making it easier for the victim to discover that they might have a malicious program on their computer.
  + Victim machine will need libraries such as python and pynput installed to cause our program to work.
  + Did not implement
    - Logging what app, the keystrokes were made in
    - Length of keypress
    - Clipboard of the keystrokes

**Improve in future**

* + It would be ideal to have the keylogger also send what application the keystrokes are made in so that the attacker has more information to exploit. It would also be ideal to send a message indicating every time the user switched to an application.
  + Knowing the length of a keypress would improve the transparency of the key logs for the attacker
  + Save clipboard text
    - hardest part would be logistics: how do you make it easily readable in the email? Do you send a new email when the clipboard text changes? What about clipboard files or images?
    - This would allow the attacker to obtain even more vital information if the above logistic questions were solved.
  + Alternate idea for taking screenshots: Perhaps we could use pynput to press the PrintScrn button, which saves a full screenshot (all monitors) to clipboard.
  + Having the screenshots hidden or deleted after capture would be more ideal in hiding the malicious program
    - maybe there is a way to attach image data with MIMEImage without it being saved to a file. If not, then there must be a way to create a temporary file that is able to be deleted while the keylogger is still running.
  + Convert from python program to an executable to allow the malicious program to be run on any computer regardless of whether the victim’s computer had python or not
  + Find a way for the key logger to not be detected by an antivirus program so that it can run on a protected computer