Project Report: Key Logger

By: Dan Sutter, Lauren Potersnak

Objectives

- Create a keylogger
  - Records victim's keystrokes
  - Screen captures the victim's screens
  - Records what program the victim is using
  - Sends the keystrokes 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

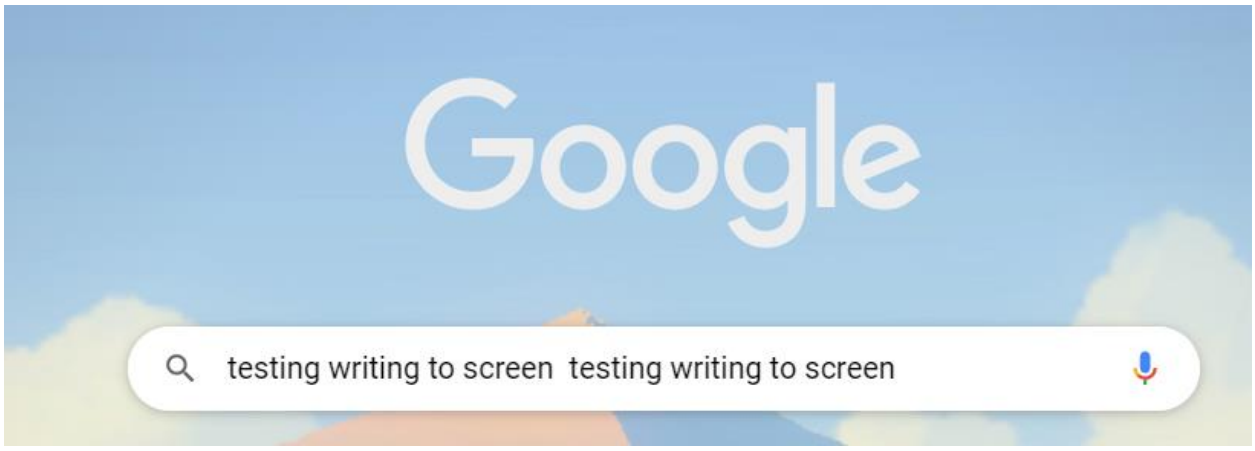
- Key_logger gets activated either by clicking on the pyw file or by attaching it to a trusted program with launch.bat
- The Key_logger.pyw runs in the background and periodically sends emails to the email address set up for it
- Keys are logged with on_press function and emailed with smtplib.SMTP_SSL
- Logged keystrokes are made readable by removing 'Key.' and implementing a way to account for spaces and backspaces, and by enclosing special keys in brackets

Implementation

- Implemented with python version 3.9 using smtplib and pynput libraries
- The .pyw extension is used instead of .py to hide when the program is running on an unprotected computer
  - If the normal .py extension was used, then a window would display, alerting the user to the program's existence
- Our logger records the victim's keystrokes
  - Works with QWERTY layout keyboards and Windows on-screen keyboard; Untested on others
- Our logger sends screenshots of the victim's computer screen
- The attacker obtains keystrokes and screenshots through email – the keylogger 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 the trusted program Internet Explorer whenever the victim selects the Internet Explorer shortcut

Output

- Sample output of only keystroke capture

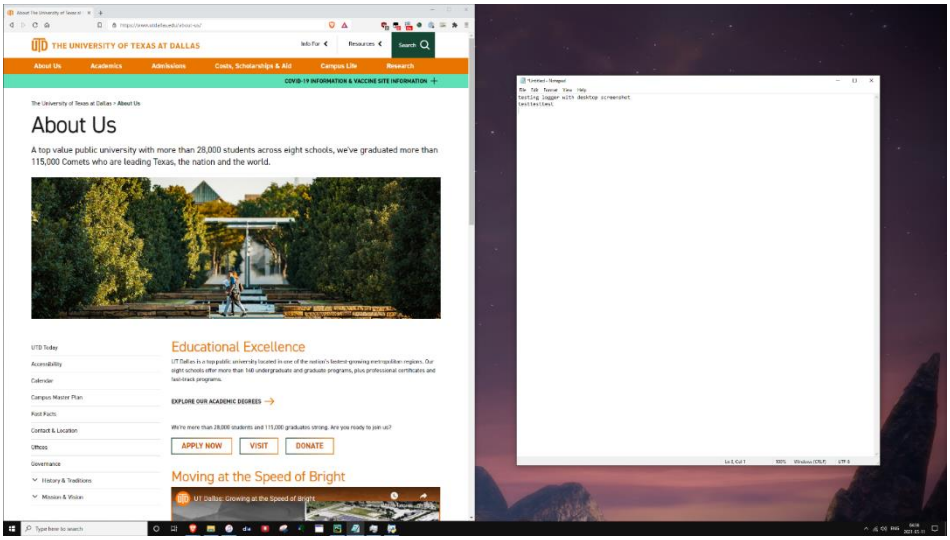


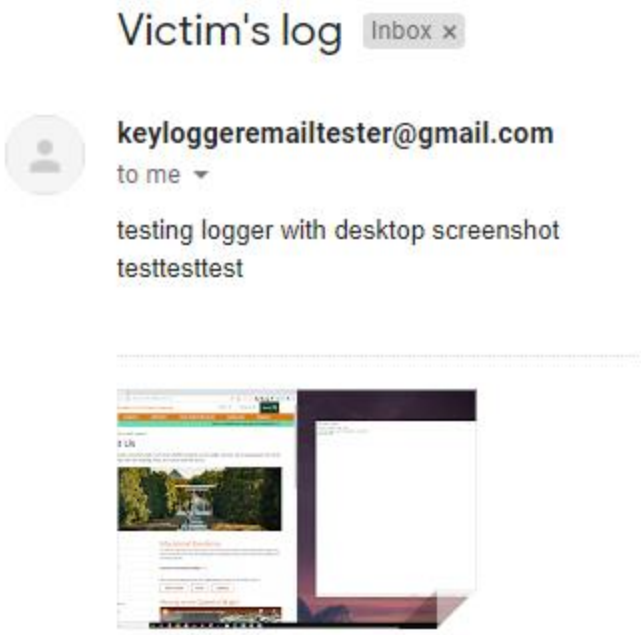
Key Logger <keyloggeremailtester@gmail.com> 4:45 PM (0 minutes ago)
to me

testing writing to screen testing writing to screen

Reply Forward

- Sample output of keystrokes and screenshot





Challenges

- We could only test our keylogger with the default QWERTY layout for physical keyboards and with the Windows On-screen 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 not completely comfortable with python. The screenshots that we were able to take only capture the main monitor, so additional monitor captures would be missed – making our keylogger less effective than we would like. The screenshots are also not deleted from the victim's computer, making it easier for the victim to discover that they might have a malicious program on their computer.
- The victim's machine will need libraries such as smtplib and pynput installed to enable our program to work.
- Did not implement
    - Logging what application the keystrokes were made in
    - Length of keypresses
    - Copying information from the victim's clipboard

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
- Saving clipboard text

        - The 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.
    - An alternate idea for taking screenshots: Perhaps pynput could be used to press the PrintScrn button, which saves a full screenshot (all monitors) to the clipboard.
    - Having the screenshots hidden or deleted after capture would be more ideal in hiding the malicious program
        - There may be a way to attach image data with MIMEImage without it being saved to a file. This would tie in nicely with our program pressing PrintScrn, if clipboard images can be directly manipulated. 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 a python program to an executable to allow the malicious program to be run on any computer regardless of whether the victim's computer has python and/or the required libraries
    - Find a way for the key logger to not be detected by an antivirus program so that it can run on a protected computer