# KEYLOGGER/ PHISHING

CMSC 414 SPRING 2019

VINCENT NGUYEN

# WHAT IS A KEYLOGGER?

A keylogger is sometimes called a keystroke logger or system monitor

It is a type of surveillance technology used to monitor and record each keystroke typed on a specific computer's keyboard

The recording is done typically in a covert manner so that you don't know that your actions are being monitored

There are even keylogger software that is available for use on smartphones

# WHAT IS ITS USE?

Keylogger recorders may be used by employers to observe employees' computer activities

It can be used by parents to supervise their children's internet usage

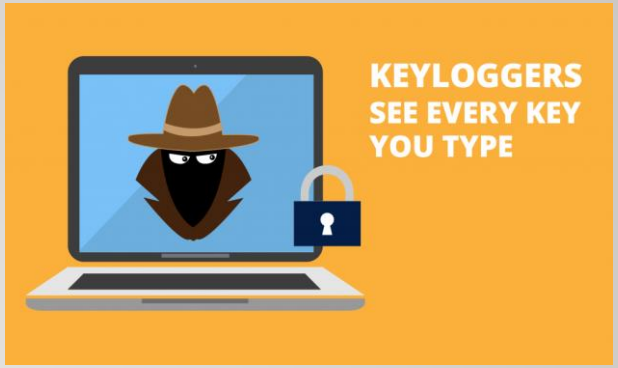
Keyloggers can be a tool for users to track possible unauthorized activity on their devices.

Law enforcement agencies can use it to analyze incidents involving computer use.

# HOW CAN IT BE EXPLOITED?

- Keyloggers are often used as a spyware tool by cybercriminals to steal personal information, login credentials, and other sensitive data
- Cybercriminals can get PIN codes and account numbers for your financial accounts
- They can steal passwords to your email and social networking accounts and then use this information to take your money
- It can be used to steal your identity and possibly extort information and money from your friends and family.

# HOW CAN YOU GET ATTACKED?




- Keyloggers spread in much the same way that other malicious programs spread.
- Most keyloggers are installed on your system when you open a file attachment that you received via email, text message, P2P networks, instant message or social networks
- Keyloggers can also be installed just by you visiting a website if that site is infected
- Lastly, keyloggers can purchased and installed in person if they have access to the victim's computer

# MY OBJECTIVES

- I will create two separate keyloggers:
  - A keylogger that would be sent via email to record the keystrokes of the victim and then the information would be sent via email back to myself
  - A keylogger that would run silently in the background of a victim's computer that would save the recordings into a text file. It would launch automatically without the victim knowing.

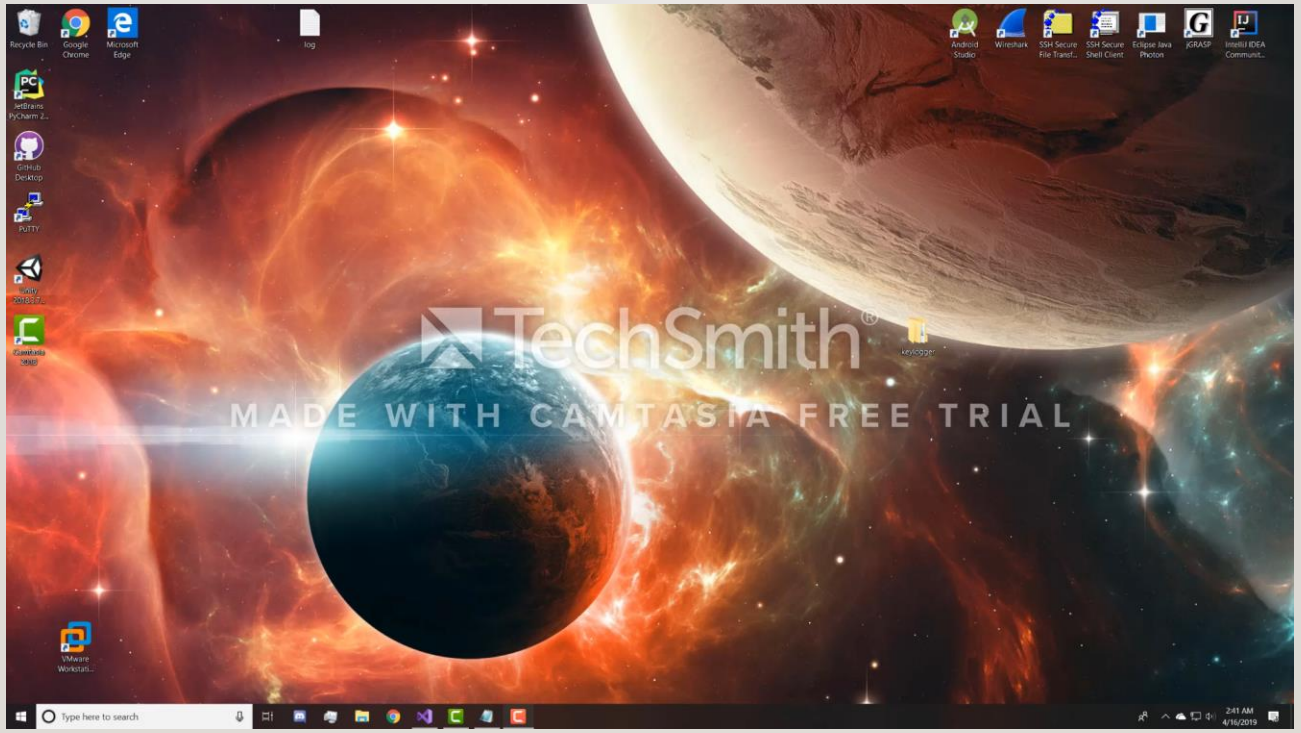
# TASKS AND APPROACH

- Research on keylogging and phishing – Getting adequate background information on keylogging and how it has been used. Also find out about any big cyber-attacks that involved keylogging.
- Create a keylogging application – Make an application that would look like a normal application that users would use often. (Ex. A game login interface, or a bank account)
- Write the code for keylogging application – Write the code needed to record keystrokes of a victim who opens the fake application page and enters information.
- Test the application and fix any bugs – Make sure that the keylogger works as intended and make sure that it looks as realistic as possible.
- Create a keylogger for a desktop – Write the code for a more advanced keylogger that the victim would unknowingly have running in the background logging all keystrokes entered.
- Getting the keylogger to launch – Finding out how to get the keylogger to launch whenever the victim is using the desktop.
- Create a detailed presentation – From all the gathered research and knowledge gained from the project, create a slide presentation in pdf format.
- Create a demo video – Make a video that shows how keylogging works and how it can affect a user. Explain what keylogging can do and show an example of it running.

# IMPLEMENTATION

- Email Sending Keylogger
  - Using Visual Basic to create a keylogger
  - Keylogger will record what is typed from the keylogger's email
  - It would send an email to the attacker's email periodically of what is typed along with time/date
- Hidden Keylogger
  - Using Python to create a keylogger
  - Keylogger would launch whenever the user was to open their web browser
  - It would record anything that is typed in and would save it to a text file
  - The program would run hidden without the victim noticing
  - This would work if the attacker had access to the victim's computer

# DEMO VIDEO


Recycle Bin
Google Chrome
Microsoft Edge
log
Android Studio
Wireshark
SSH Secure File Transf...
SSH Secure Shell Client
Eclipse Java Photon
jGRASP
IntelliJ IDEA Communit...
NetBeans PyCharm 2...
GitHub Desktop
PUTTY
keylogger
VMware Workstati...
TechSmith
MADE WITH CAMTASIA FREE TRIAL
Type here to search
2:41 AM
4/16/2019

# EVALUATION RESULTS

- I learned from this class project about the dangers and misuse of programs like keyloggers
- It can be very harmful if used by cybercriminals because they can retrieve information regarding things like bank accounts and personal login credentials
- From the keyloggers I created, the email sending keylogger was able to send an email to the attacker's email every 60 seconds once the program had started
- The victim was shown no sign that their keystrokes were being recorded
- In the hidden keylogger program, I was able to get the program to launch using a bat file
- It would launch seamlessly and start recording keystrokes right away once the web browser I attached it to was opened
- There was a pop up for a millisecond that would be ignore by most users
- After that, there were no other signs that their keystrokes were being recorded
- A text file was constantly recording whatever was being typed in and the program would not end unless closed from Task Manager

# SOURCES


- https://securingtomorrow.mcafee.com/consumer/family-safety/what-is-a-keylogger/
- https://searchsecurity.techtarget.com/definition/keylogger
- https://usa.kaspersky.com/resource-center/definitions/keylogger