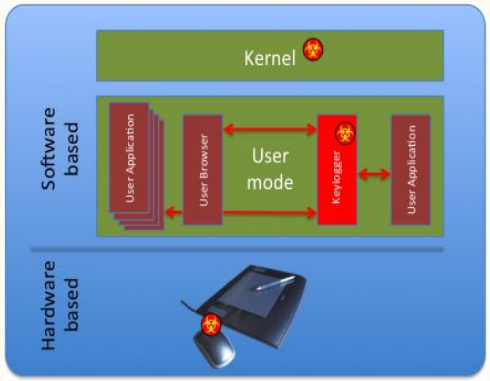
Christian McKee Tyreek Woods Quran Henry Drew Howell Timothy Williams Shane Turner

What is a keylogger?

- A keylogger is a tool used by hackers to monitor and record keystrokes on your keyboard. Some keyloggers can be difficult to detect, whether they are installed on your operating system or incorporated in hardware. Below are the different types of keyloggers.
  - Most Common Keyloggers
    - API (Application Programming Interface) Keylogger (Will be demonstrated)
    - Hardware Keyloggers
  - Other Keyloggers types
    - Form Grabbing-Based Keyloggers
    - Kernel-Based Keyloggers



API Keylogger

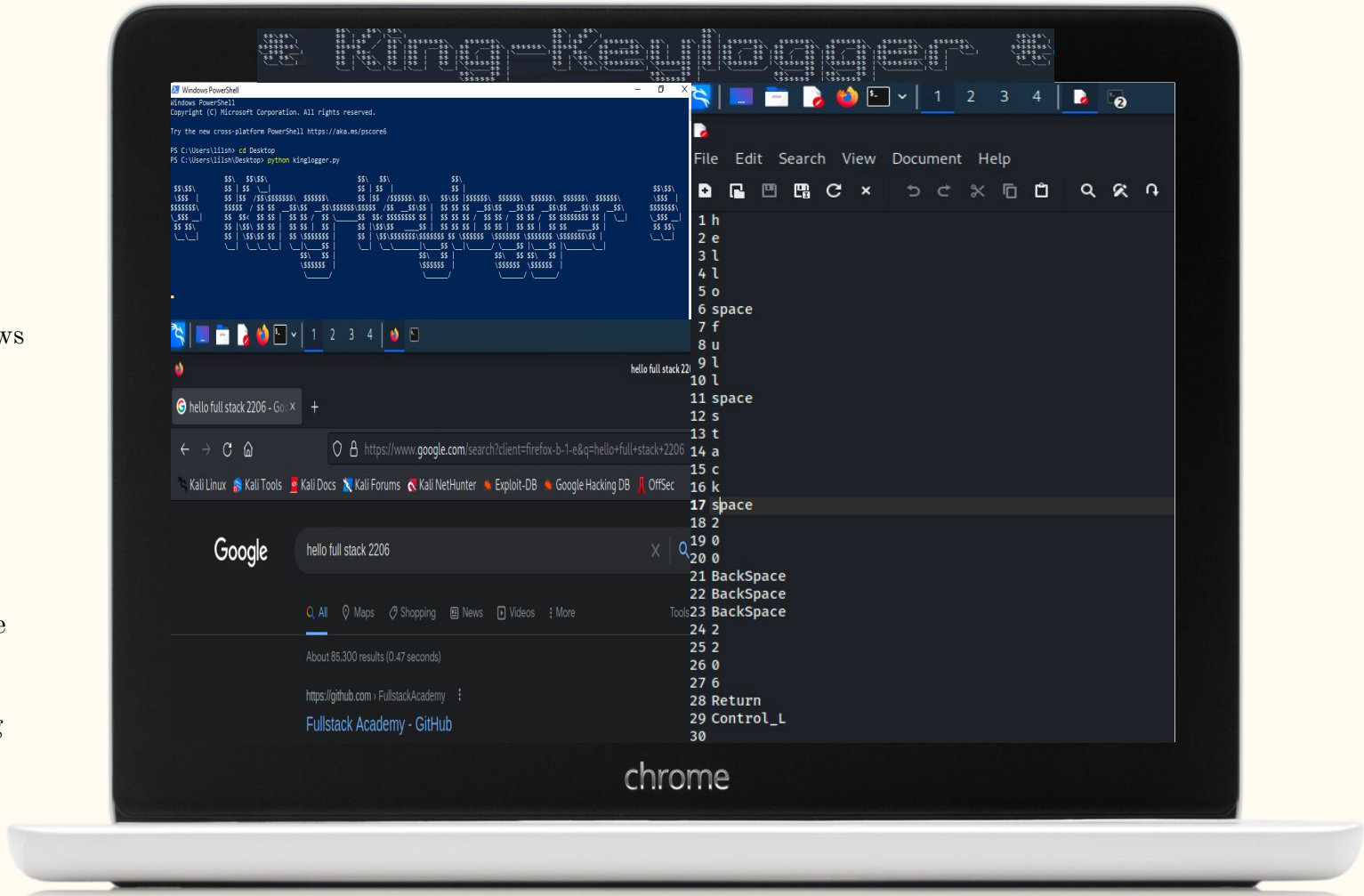
To the right is an example of an API Keylogger, updated, and edited by this group to become functional, log keystrokes and save the keystroke to designated directory.

API Keylogger Cont.

The top left corner shows the Keylogger being activated using the python3 command.

Bottom left you see the user input “hello full stack 2206”

To the right you can see a log that was saved to my Desktop that has every keystroke spelling errors and correction.

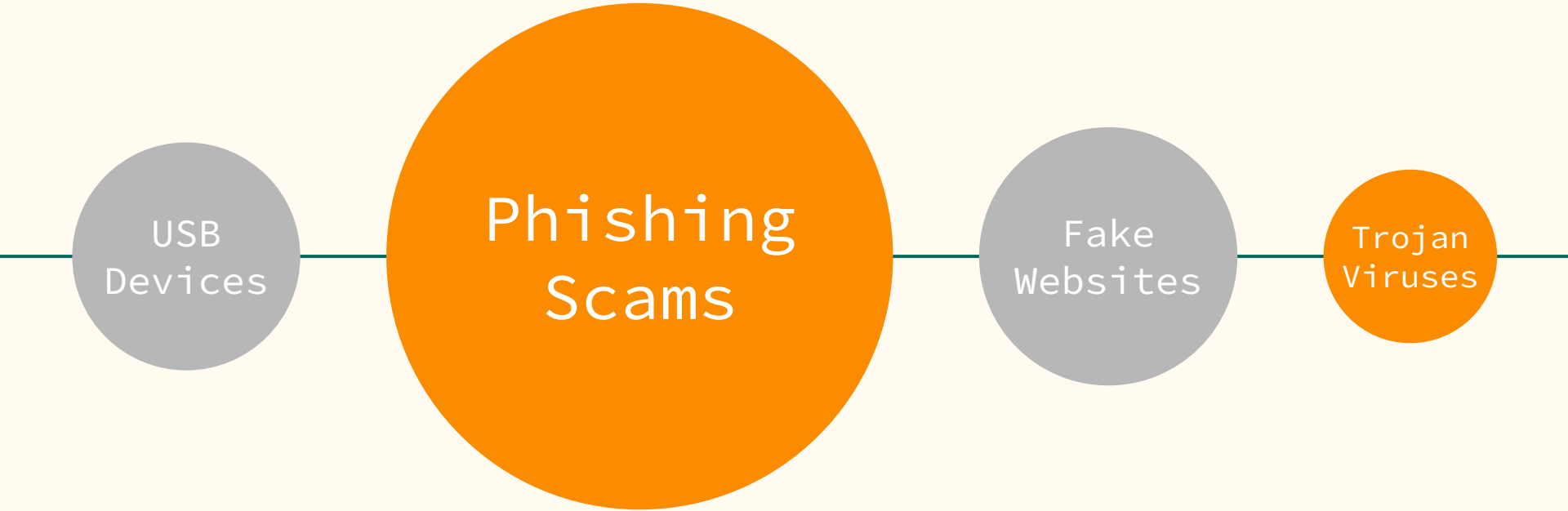


API Keylogger Cont.

The Top shows the process of turning the python file made into an executable using the tool nuitka.

The Bottom is the executable file created after the python file compiled to a .exe.

How is a Keylogger Used/Transported?



- Phishing via Email with Guerrillamail -

CONFIDENTIAL

How to utilize the Guerrillamail service in order to execute a phishing campaign via email.

⚠ *ALERT!* The following information is related to Information Security and does not promote hacking / malicious behavior / software piracy.
Do not investigate individuals, websites, servers, or a network, or conduct any illegal activities on any system you do not have permission to analyze.

- Phishing via Email -

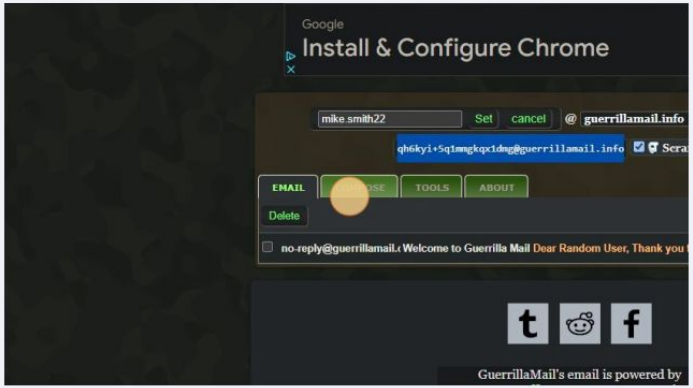
1 Navigate to https://www.guerrillamail.com/

2 Click to edit the email address username or you can leave the auto-filled data however, you may experience greater success if you can craft the email to appear as legitimate as possible.

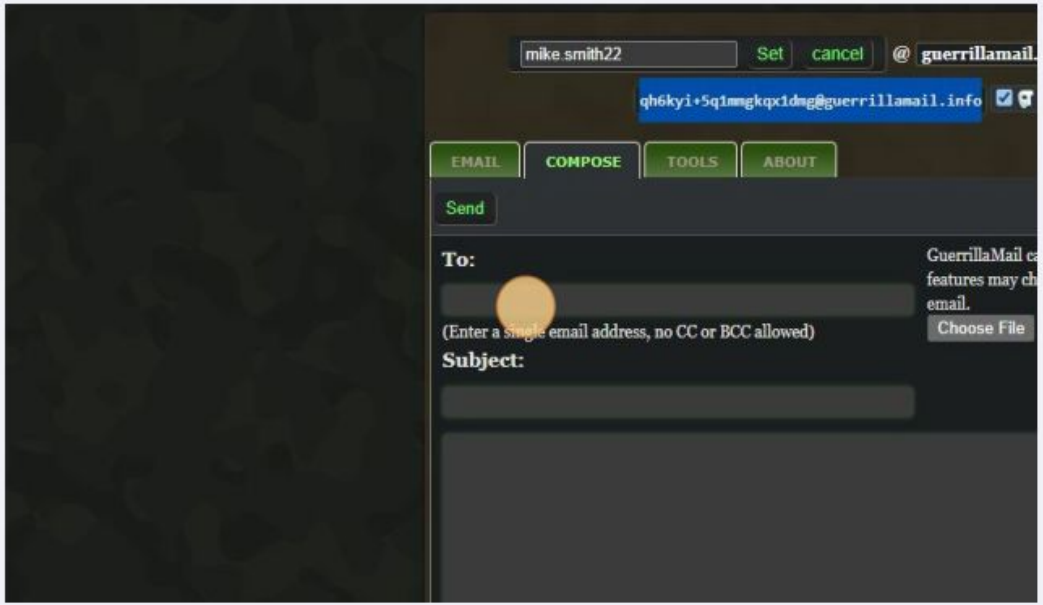
3 Enter a username; as stated before, it should be tailored specifically to the situation at hand so that it may be as convincing as possible.

4 Click this dropdown and choose a domain for the sender's email address.

5 Click "COMPOSE"

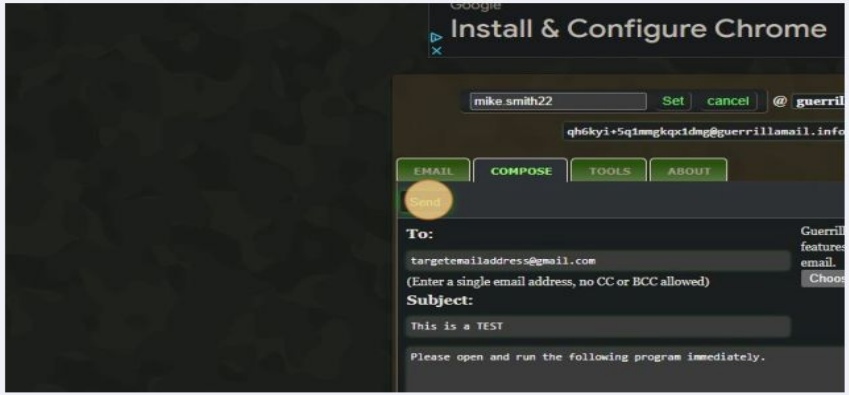


6 Click this text field and proceed to input your targets email address.

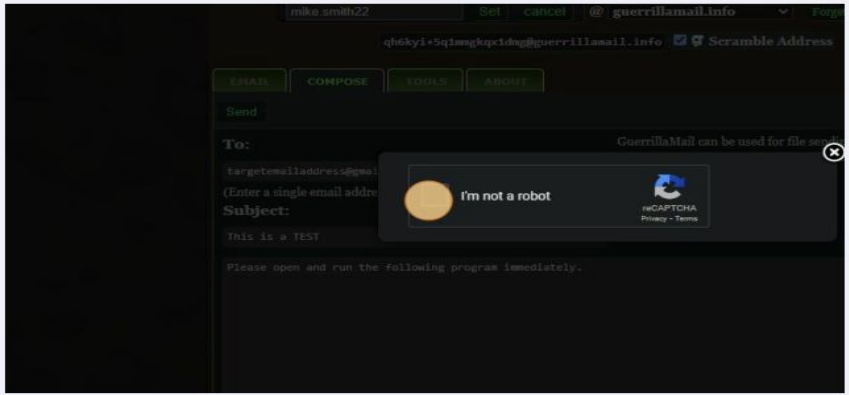


Attachments may also be sent using this service, providing the ability to exploit a system via email more easily as malware can be coupled with the email as an all-in-one payload. Again, you should draft the email as specific to your target as possible so you may have a greater chance at a successful phishing campaign.

7 Click this button to send the email.



8 Click this box to fulfill the CAPTCHA then, to verify the email has been sent, you should receive a message at the top of the website stating "Message dispatched".

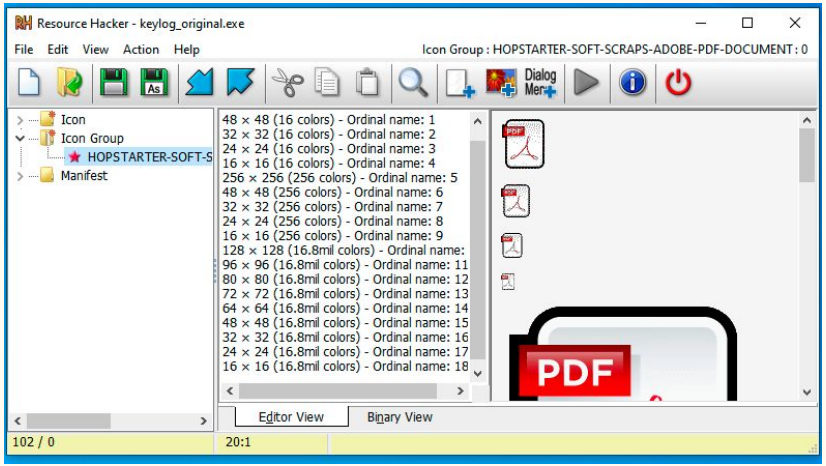


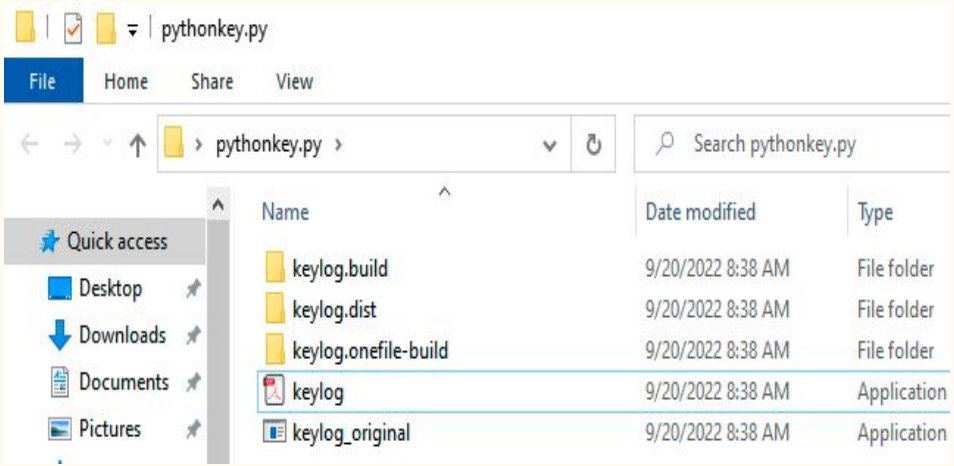
- Common Phishing Techniques and Examples -

10

⚠ Some of the most common techniques used in phishing attacks include the following: Big discounts and limited supply - 'Demands' from leadership of which will more often that not, attempt to spark a sense of urgency and the need to act immediately - Deceptive techniques to trick users into clicking a malicious link that will then redirect them to a website designed to steal their personal information - Malicious links to trigger the automatic download of malicious software on victims' device(s).

LIVE EXAMPLE - - - - - - GONE PHISHING

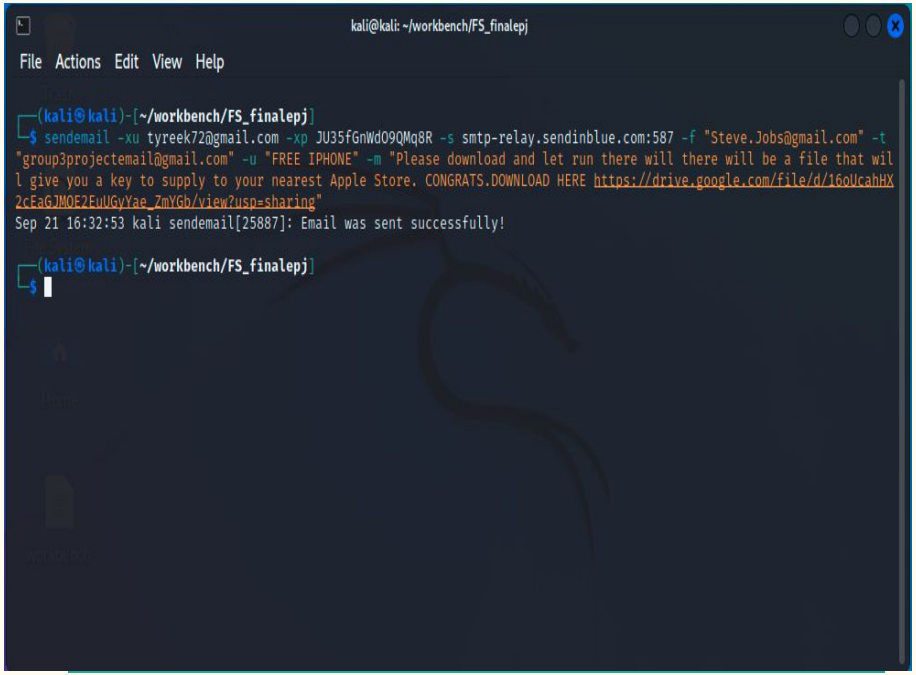


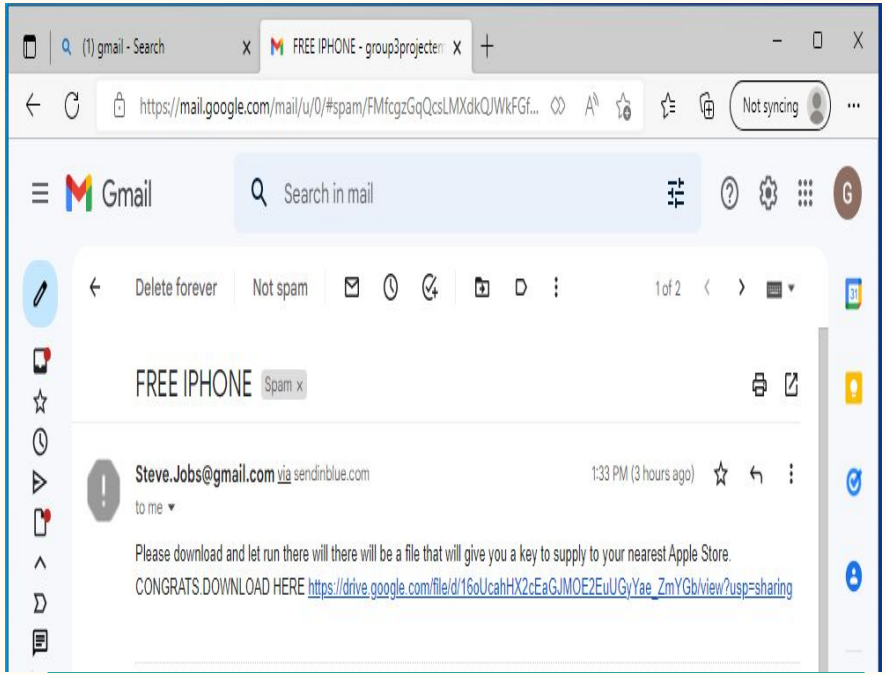


RESOURCE HACKER

Above the hacker uses a tool called resource hacker that allows them to spoof the icon of the file to make the user believe it is a trusted pdf.

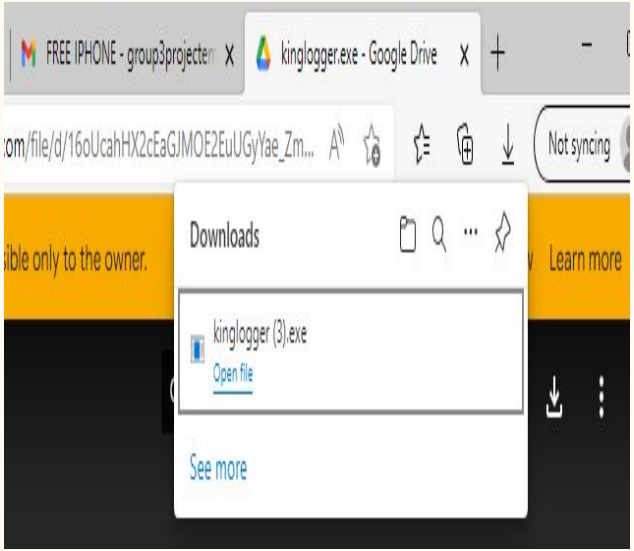
LIVE EXAMPLE - - - - - - GONE PHISHING

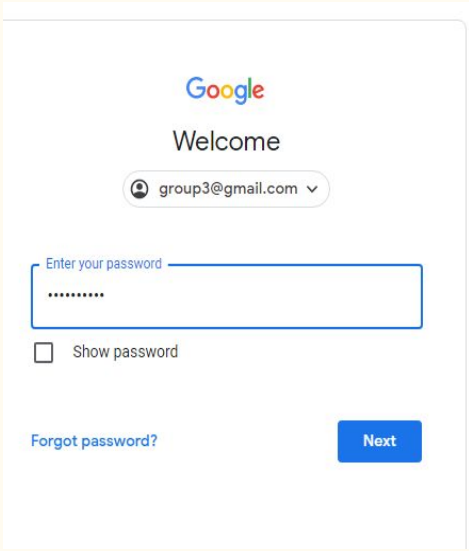


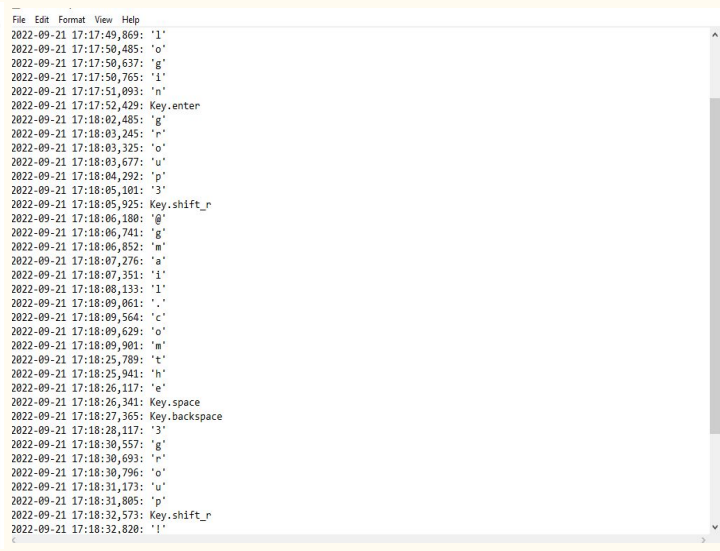


In this part of the phishing attempt you can see the hacker spoofing his/her email to Steve.Jobs@gmail.com and targeting the user Group3projectemail@gmail.com offering them a free iphone if the victim downloads a key to provide to the apple store.

LIVE EXAMPLE - - - - - - Keylogger In Action



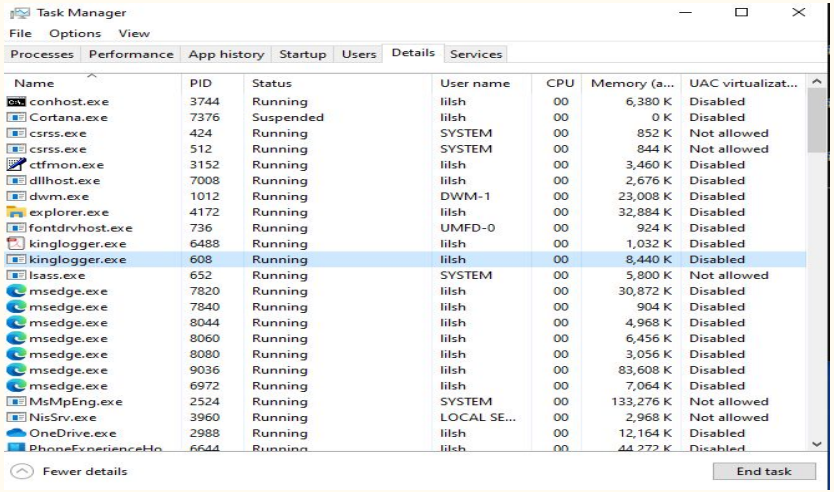


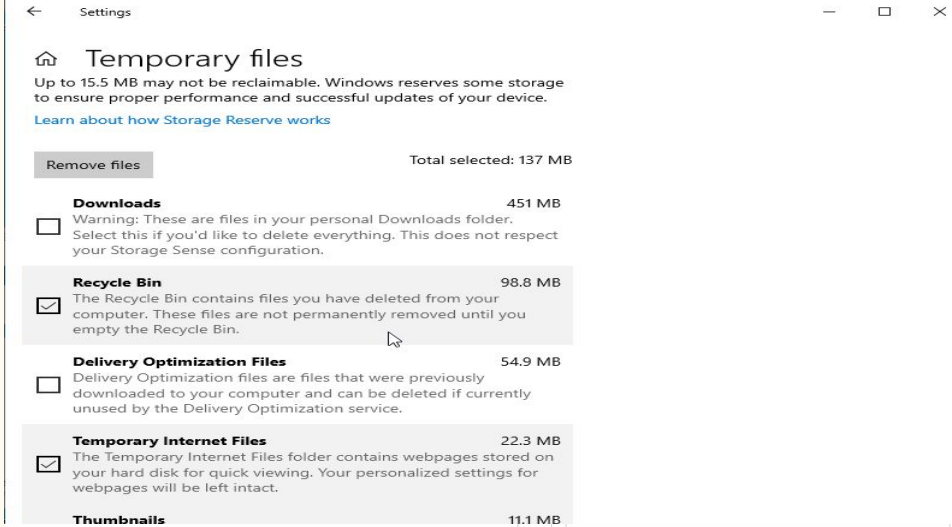


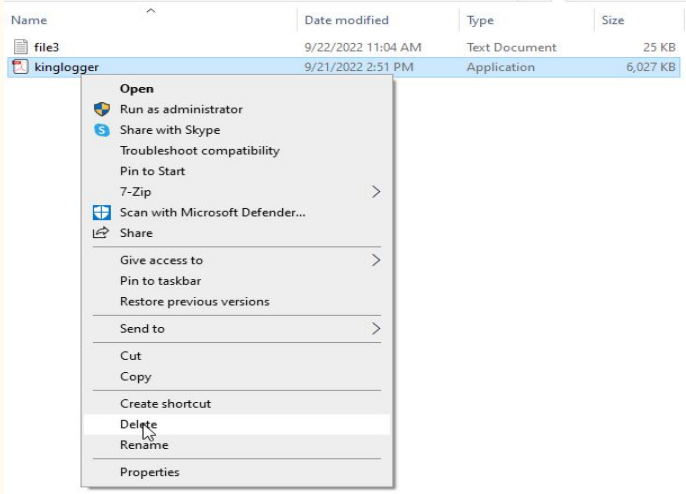
Finally the logger is on the victim's computer and will begin recording all keystrokes and will relay this information back to the hackers devices as a .txt file.

GONE PHISHING CONT.

Detecting the malicious program can be done using windows task manager, where we will see the program running as a background process.
We can Force Stop the program to terminate the executable script.
Removing the program from your system can be done by using uninstall programs in the control panel.
You should also delete all associated files and empty the recycling bin.





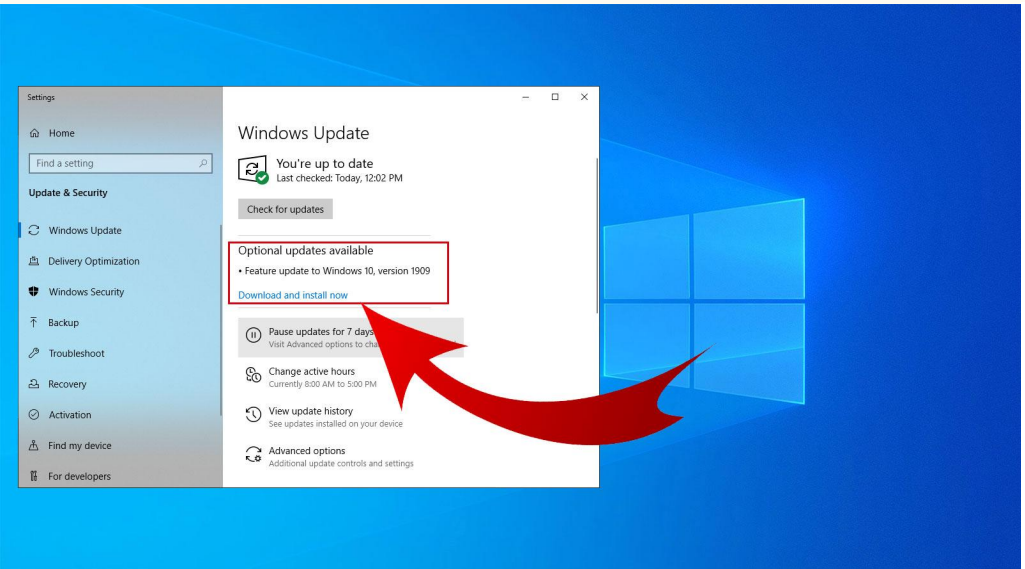


Protecting yourself from keyloggers

The best way to protect yourself is to be vigilant:

- Keep an eye out for misspellings, inconsistencies, and other small oddities in text and addresses.
- Think before you click—hover over links to confirm they'll take you to where you're expecting to go.
- When in doubt, check with the supposed sender before you take action.
- Immediately report any suspicious activity to your IT team so they can take action ASAP.
- Keep your team abreast of the latest forms of social engineering—they change rapidly, so that's what we'll dive into next…

- Avoid using public internet services such as Internet cafés if at all possible.
- Don't install software of doubtful source,
- Be careful when you log on to a computer that does not belong to you! If it is a computer with free access, quickly examine the configuration, before connecting to sites asking for your password, to see if users have gone before you and if it is possible or not for an ordinary user to install the software.
- In case of doubt, do not connect to any secure sites for which there is a stake (online banking, …)




SUMMARY
chrome

For Educational Purposes Only

For Educational Purposes Only

National Cybersecurity Awareness Month – October 2022

For Educational Purposes Only

For Educational Purposes Only