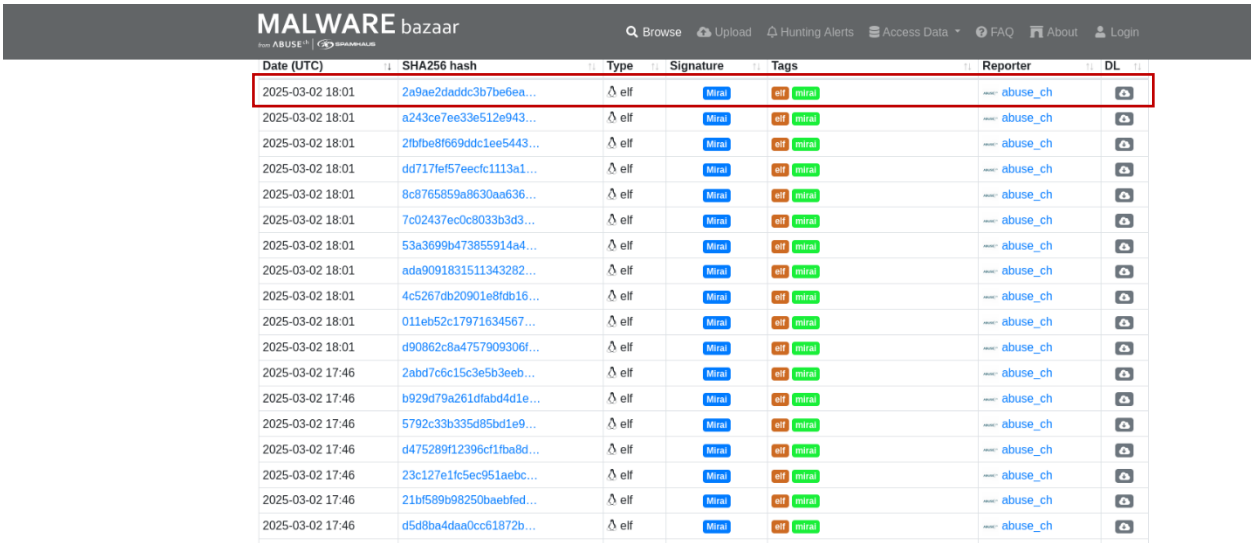
Nick Carpenter
Old Dominion University
CYSE 450: Ethical Hacking and Penetration Testing
Lab 3: Malware Analysis
Handout Date: February 27, 2025
Due Date: March 07, 2025, 11:59 pm
Total Points: 30

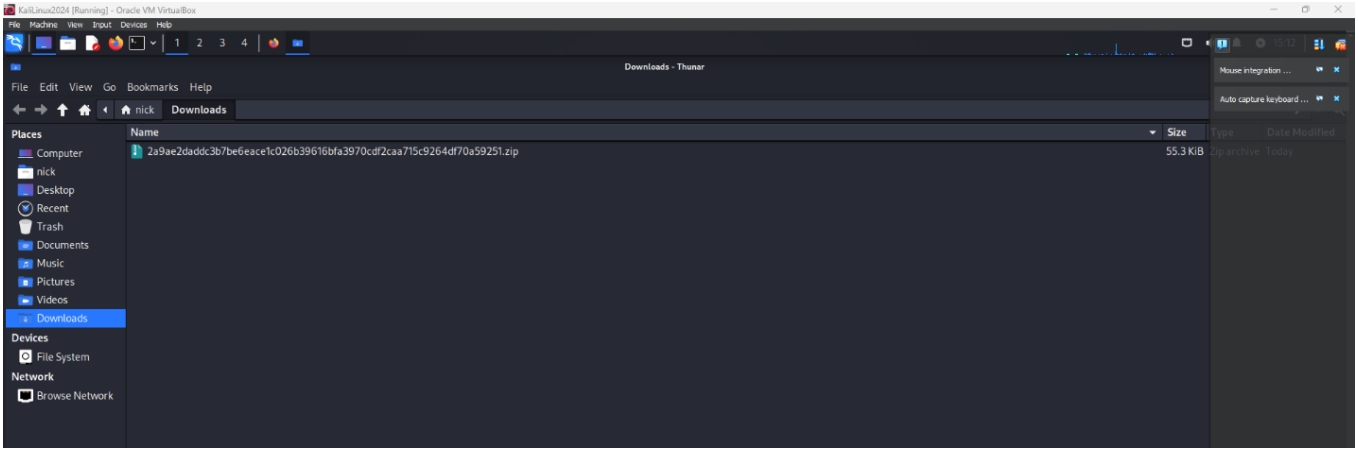
Tasks

Task-1: Go to https://bazaar.abuse.ch/browse/ and select a malware with the “Mirai” signature. Use the “Signature” column to find out all the malwares with the “Mirai” signature or use the search option with the “Mirai” keyword. Take a screenshot similar to the following screenshot and make sure you highlight the malware you selected. 2 points



Date (UTC)	SHA256 hash	Type	Signature	Tags	Reporter	DL
2025-03-02 18:01	2a9ae2daddc3b7be6ea…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	a243ce7ee33e512e943…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	2fbfbe8f669ddc1ee5443…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	dd717fef57eecfc1113a1…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	8c8765859a8630aa636…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	7c02437ec0c8033b3d3…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	53a3699b473855914a4…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	ada9091831511343282…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	4c5267db20901e8fdb16…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	011eb52c17971634567…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 18:01	d90862c8a4757909306f…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 17:46	2abd7c6c15c3e5b3eeb…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 17:46	b929d79a261dfabd4d1e…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 17:46	5792c33b335d85bd1e9…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 17:46	d475289f12396cf1fba8d…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 17:46	23c127e1fc5ec951aebc…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 17:46	21bf589b98250baebfed…	elf	Mirai	elf mirai	abuse_ch	
2025-03-02 17:46	d5d8ba4daa0cc61872b…	elf	Mirai	elf mirai	abuse_ch	

Task-2: Read the details of the selected malware and download the malware sample using the “download sample” link. Take a screenshot showing the downloaded malware sample in your computer. 2 points



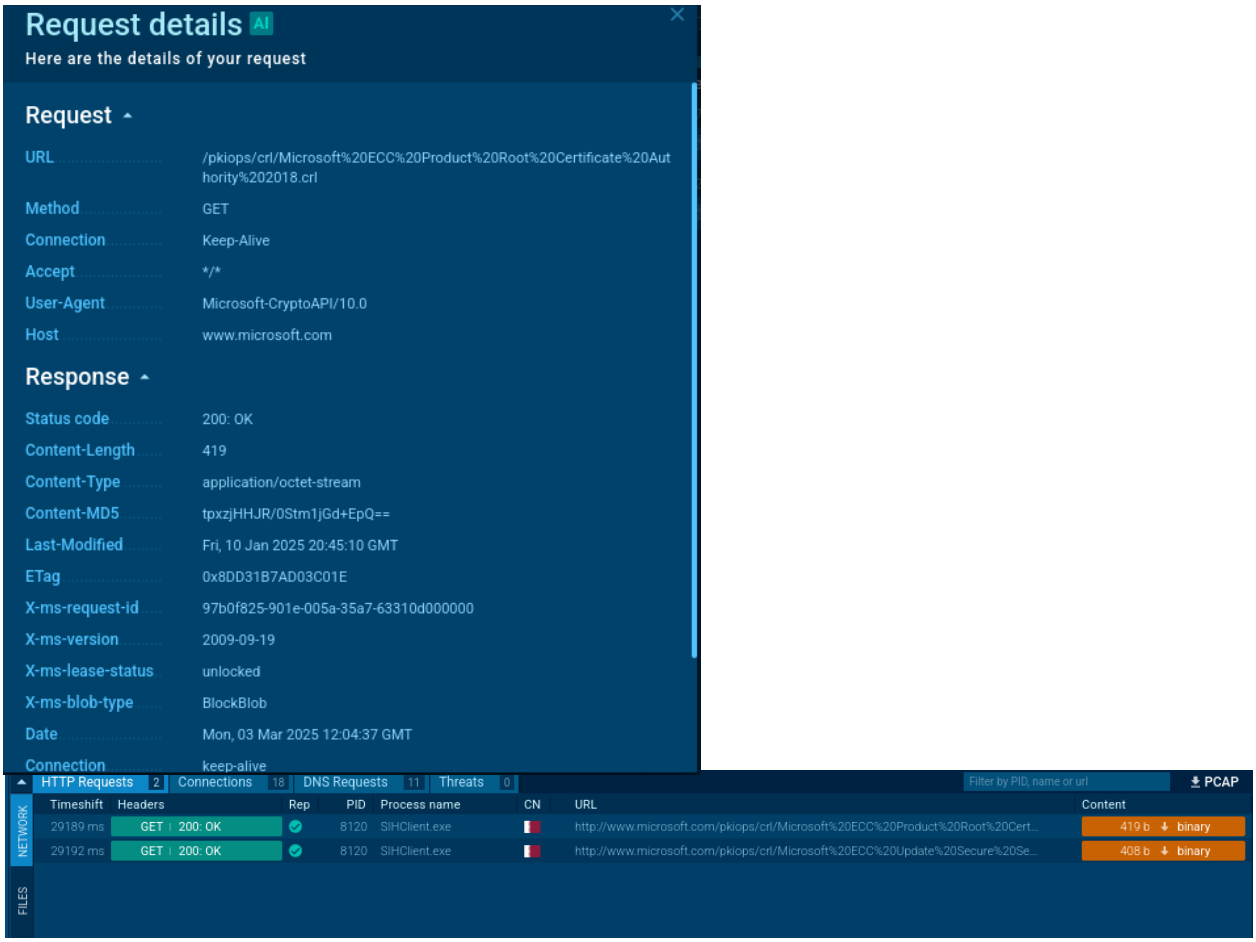
Task-3: Go to https://app.any.run/ and sign up using your odu.edu email. You will be sent a
verification link through email. Use the link to log in to the any.run dashboard.

Task-4: In any.run dashboard, choose the “Submit File / Email” option to select the previously downloaded malware sample in order to upload for the analysis.

Task-5: Once the malware sample is selected, click on the “Run a public analysis” button to upload the sample and run a malware analysis.

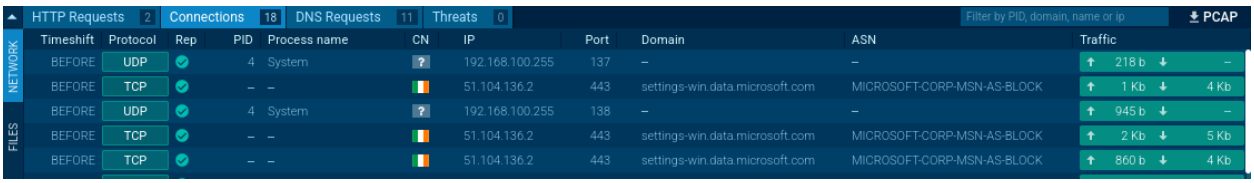
Task-6: In the bottom part of the any.run screen, you will find information about HTTP Requests, Connections, DNS Requests, and Threats under the Network tab. Here goes an
example: Go through all the information you find for each category (i.e., Http Requests, Connections, DNS Requests, and Threats) and take at least one screenshot showing information from each category. 8 points

HTTP Requests and details:

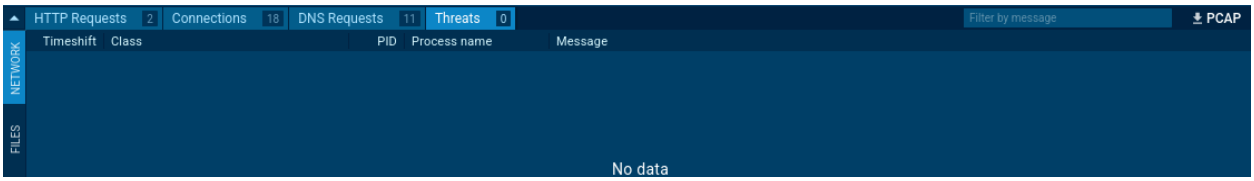


DNS Requests:

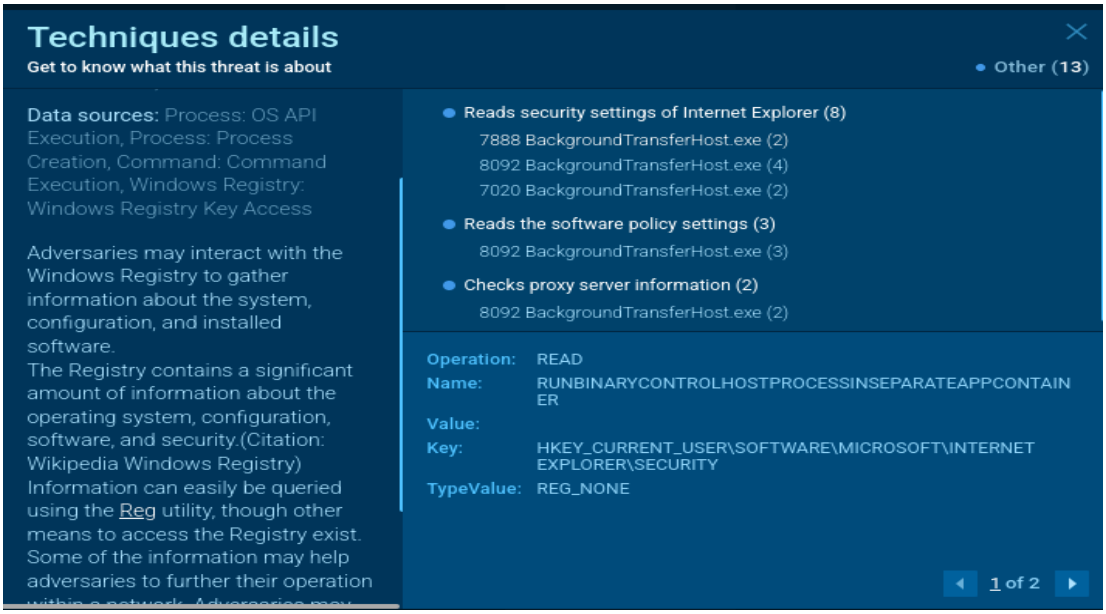
Connections:



Threats: (no current threats)



Task-7: Explore information found in the IOC, Text Report, Graph, and ATT&CK tabs on the right side of the screen. Take necessary screenshots showing any interesting finding. 3 points



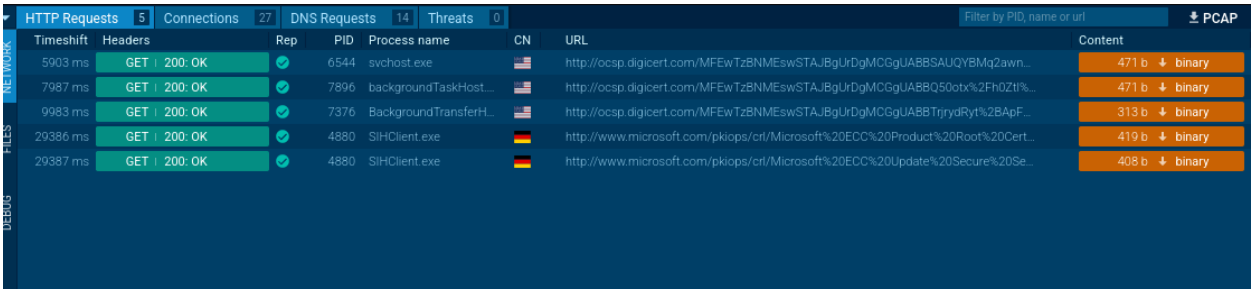
Explanation: ATT&CK provides an overview of the malware and the threats associated with it. In addition, the text file outlines that the malware will create folders in the user directory to help gain access for remotely controlling the system or other means of attack.

Task-8: Based on the information you found from Task-6 and Task-7, briefly explain the main characteristics of the malware sample. 5 points

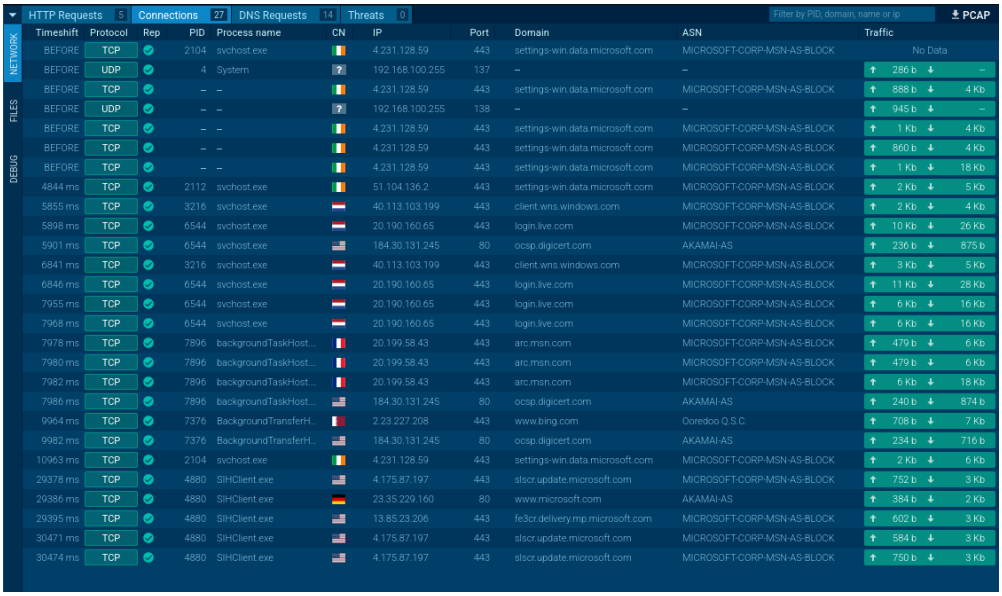
This malware interacts with the windows registry to gain information about a system to execute commands. Additionally, this malware reads security settings and creates files and folders in the user directory, performing reconnaissance. The commands executed are most commonly associated with Denial of Services attacks.

Task-9: Go to https://bazaar.abuse.ch/browse/ again, but this time, select a malware sample with the “VIPKeylogger” signature. Perform malware analysis repeating Task-3 to Task-7. Based on your analysis, explain the main characteristics of this malware sample. 5 points

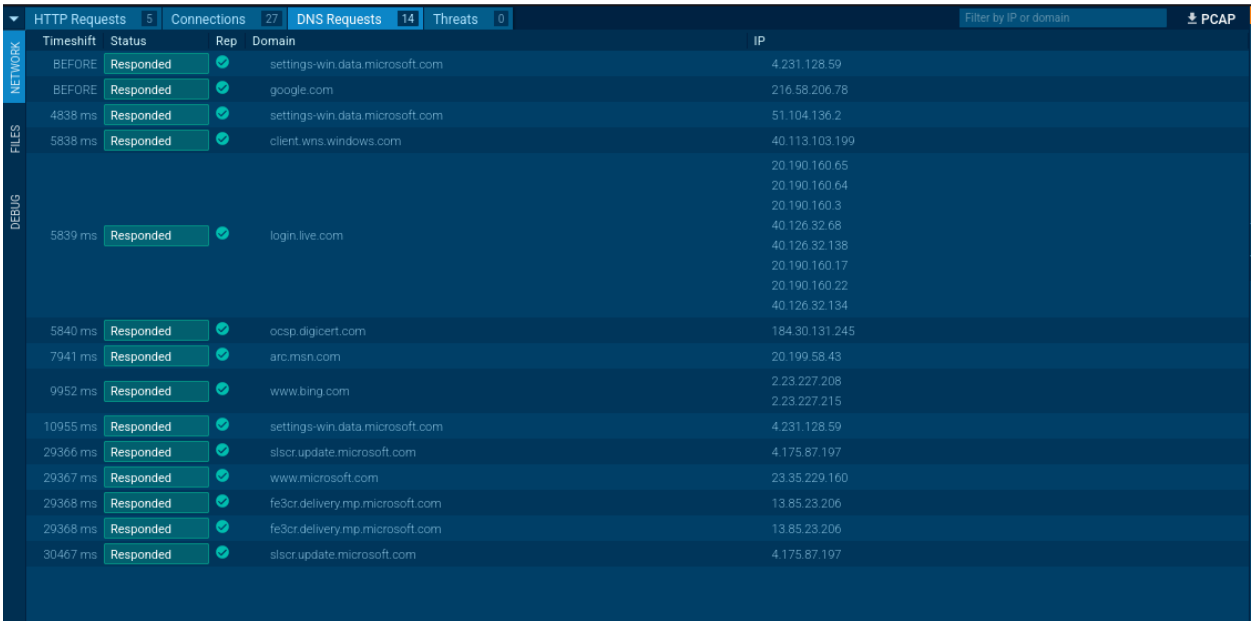
Keylogger HTTP Requests:



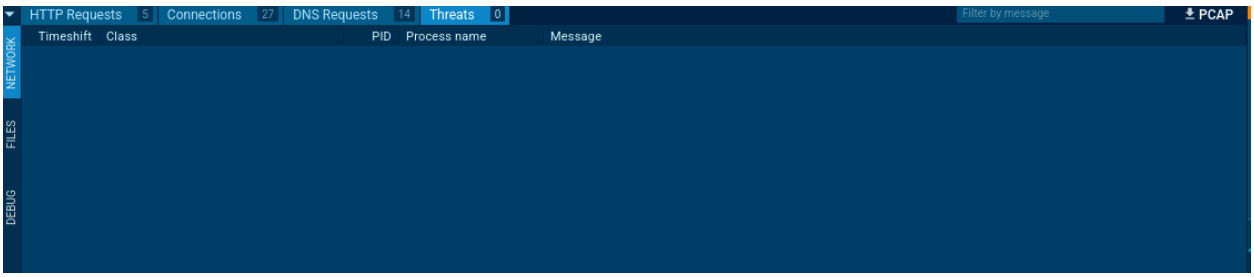
Keylogger Connections:



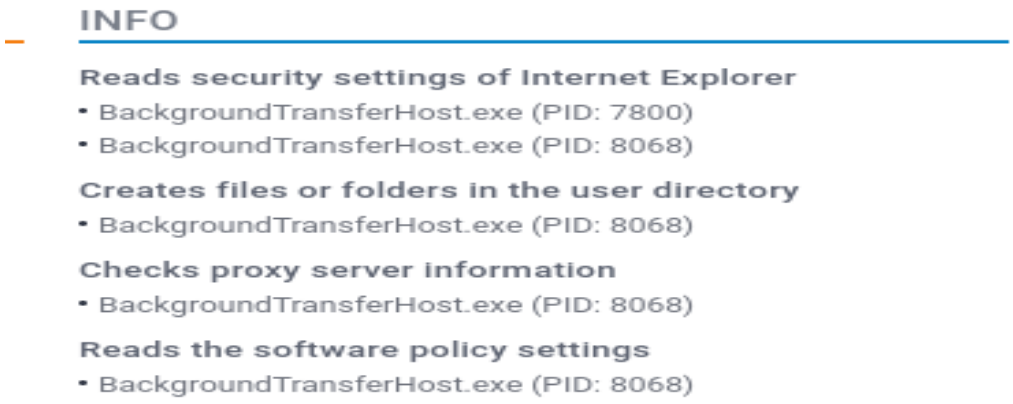
Keylogger DNS Requests:



Keylogger threats:



Explanation: This is the text report for the VIPKeylogger signature. This shows information about what the keylogger does when interacting with a system. The keylogger, is reading security settings, creating folders in the user directory, checking proxy information, and reading software policies. This is all essential for transferring sensitive information out of a network.



Task-10: Discuss the difference between Mirai and VIPKeylogger malwares in your own words. 5 points

Mirai is malware that can produce a wide variety of threats by utilizing the system data from the windows registry. This information can be useful for several hackers, including organized crime and nation states. System information can help hackers achieve executable commands on the user's system, achieve lateral movement on a network to infect other systems, and temporarily take systems offline.

VIPKeylogger create background transfer for files/folders, proxy information, security settings, and software policies and settings. This information is primarily used for credential farming. Credentials that can be transferred to an attacker may include banking information, passwords, pages visited, etc. However, credential farming is usually only used for monetary gain rather than attempting to take a system offline or infect other systems.

Turn-in Submit all the screenshots and explanations highlighted using the yellow background.