1. In analyzing the malware's behavior after the initial intrusion, it's crucial to understand where it attempts to establish persistence or further infection. Where were the files dropped by the malware located within the system's file structure?

Answer: **C:\Users\Administrator\AppData\Local\Temp**

2. The malware's communication with external servers is key to its operation. What is the URL that was used by the malware to download a secondary payload?

Answer: **https://windacarmelita.pw/picdir/big/113-1131910-clipart.svg**

3. Understanding the malware's defense evasion techniques is essential for developing effective detection strategies. What encryption technique is employed by the malware to conceal its activities or payloads?

Answer: **Rabbit**

4. Decrypting payloads is a common technique used by malware to evade initial analysis. What is the decryption key used to unlock the second stage of the malware?

Answer: **dfshji349jg843059utli**

5. Malware analysis often involves tracking how it interacts with the filesystem. What is the name of the file created by the malware to store decrypted data?

Answer: **mokpp9342jsOUth.dll**

6. Analyzing the malware's execution flow is crucial for understanding its impact and behavior. What function does the malware execute within the DLL to perform its malicious activities?

Answer: **NormalizeF**

7. Investigating related artifacts can provide insights into the broader campaign. What is the name of another JavaScript file that utilizes the domain identified during the investigation?

Answer: **sdfhui2kjd.js**

8. Attribution is a critical aspect of threat intelligence. Can you identify which Advanced Persistent Threat (APT) group is likely behind this attack?

Answer: **UAC-0057**

9. What is the country of origin associated with the APT group identified in this investigation?

Answer: **Belarus**