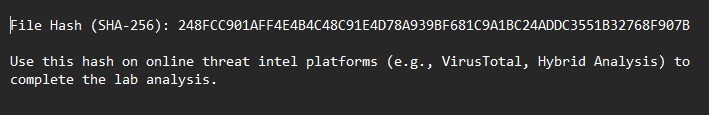
### **Red Stealer Lab — CyberDefenders**

**Scenario:** You are part of the Threat Intelligence team in the SOC (Security Operations Center). An executable file has been discovered on a colleague’s computer, and it’s suspected to be linked to a Command and Control (C2) server, indicating a potential malware infection.  
Your task is to investigate this executable by analyzing its hash. The goal is to gather and analyze data beneficial to other SOC members, including the Incident Response team, to respond to this suspicious behavior efficiently.



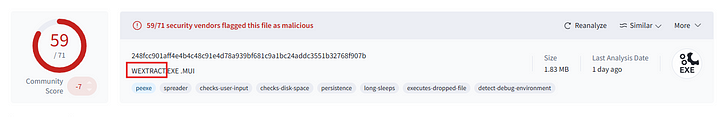
#### **Tasks**

1. Categorizing malware enables a quicker and clearer understanding of its unique behaviors and attack vectors. What category has Microsoft identified for that malware in VirusTotal?



**Answer:** Trojan

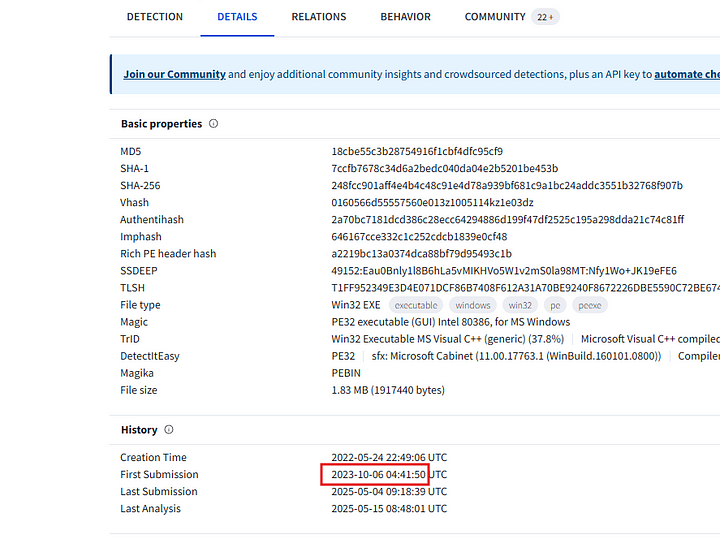
**2. Clearly identifying the name of the malware file improves communication among the SOC team. What is the file name associated with this malware?**

****

**Answer:** Wextract

**3. Knowing the exact timestamp of when the malware was first observed can help prioritize response actions. Newly detected malware may require urgent containment and eradication compared to older, well-documented threats. What is the UTC timestamp of the malware’s first submission to VirusTotal?**

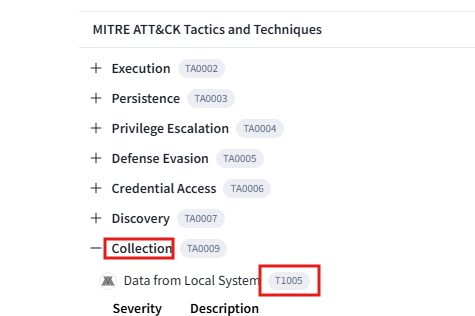
In VirusTotal, go to Details tab.



**Answer:** 2023–10–06 04:41

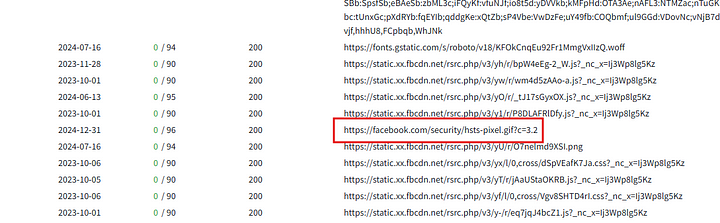
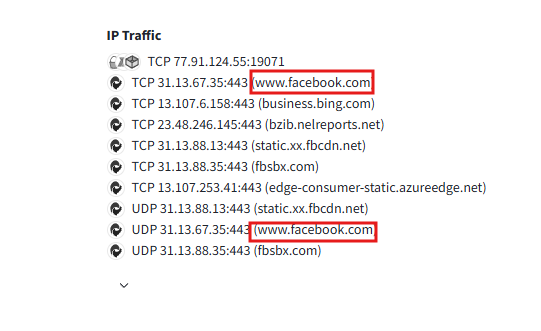
**4. Understanding the techniques used by malware helps in strategic security planning. What is the MITRE ATT&CK technique ID for the malware’s data collection from the system before exfiltration?**

In VirusTotal, go to Behavior tab and scroll to MITRE ATT&CK Tactics and Techniques section.



**Answer:** T1005

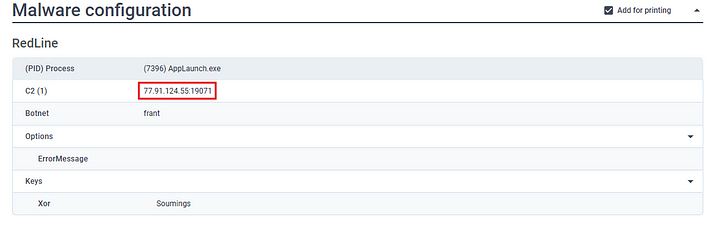
**5. Following execution, which social media-related domain names did the malware resolve via DNS queries?**

****

**Answer:** facebook.com

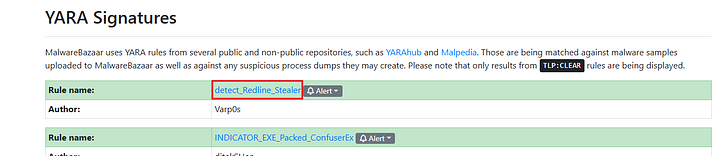
**6. Once the malicious IP addresses are identified, network security devices such as firewalls can be configured to block traffic to and from these addresses. Can you provide the IP address and destination port the malware communicates with?**

Searching on AnyRun with the given hash gave me a report. In the report the IP address and the port are listed.



**Answer:** 77.91.124.55:19071

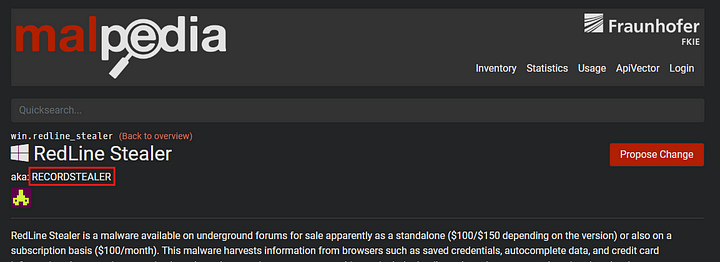
**7. YARA rules are designed to identify specific malware patterns and behaviors. Using MalwareBazaar, what’s the name of the YARA rule created by “Varp0s" that detects the identified malware?**

****

**Answer:** detect\_Redline\_Stealer

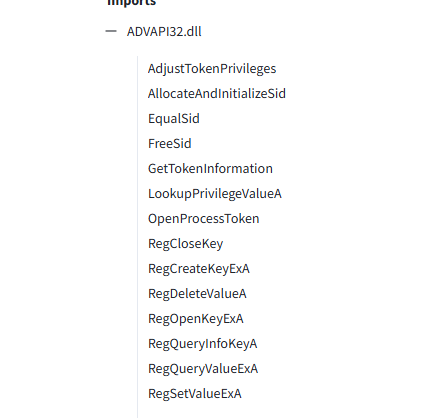
**8. Understanding which malware families are targeting the organization helps in strategic security planning for the future and prioritizing resources based on the threat. Can you provide the different malware alias associated with the malicious IP address according to ThreatFox?**

I could not find the ThreatFox report. But, Malpedia article had the malware alias.



**Answer:** RECORDSTEALER

**9. By identifying the malware’s imported DLLs, we can configure security tools to monitor for the loading or unusual usage of these specific DLLs. Can you provide the DLL utilized by the malware for privilege escalation?**

****

Many of the functions listed above are used for privilege escalatio.

**Answer:** ADVAPI32.dll

This is the end of this walkthrough.