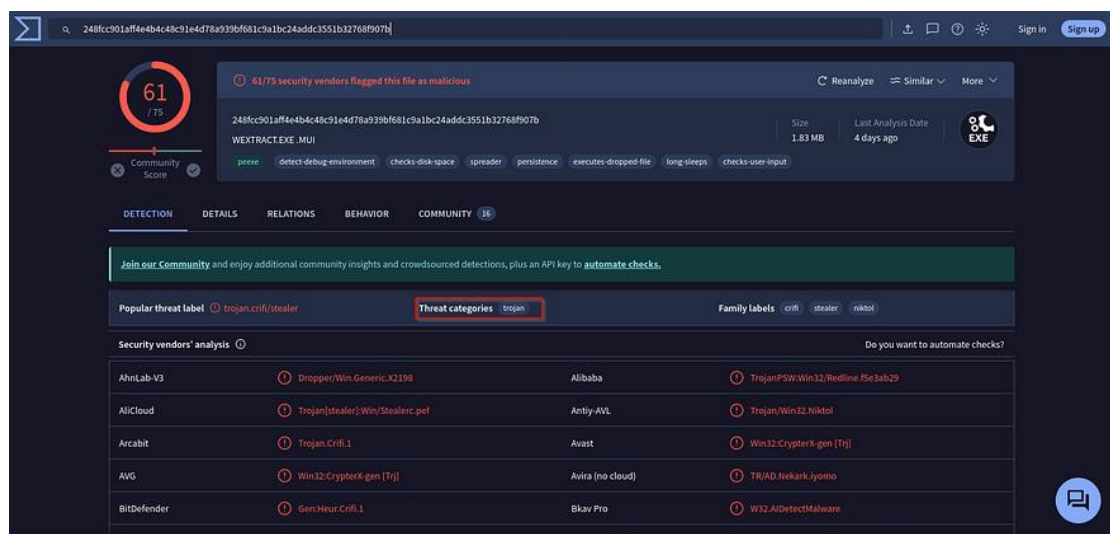


Scenario:

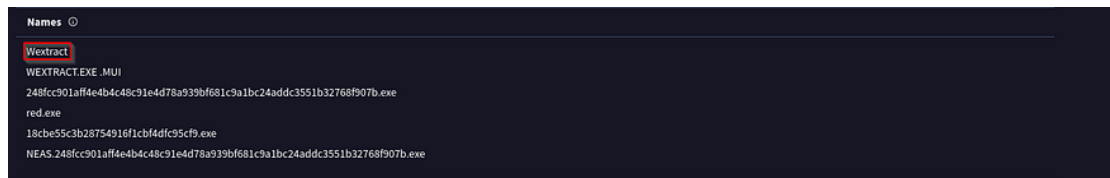
You are part of the Threat Intelligence team in the SOC (Security Operations Center). An executable file has been discovered on a colleague's computer, and it's suspected to be linked to a Command and Control (C2) server, indicating a potential malware infection. Your task is to investigate this executable 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.

Question asks what category of malware belongs to the provided hash. There are several ways to determine this, but the most straightforward is to input the hash into **VirusTotal** or a similar website. After doing so you will find the answer.



Question 1 Answer: *Trojan*

Question 2: Next, we need to find the name of the file. I stayed on **VirusTotal** and navigated to the **Details** section, where I located the file name.



Question 2 Answer: *Wextract*

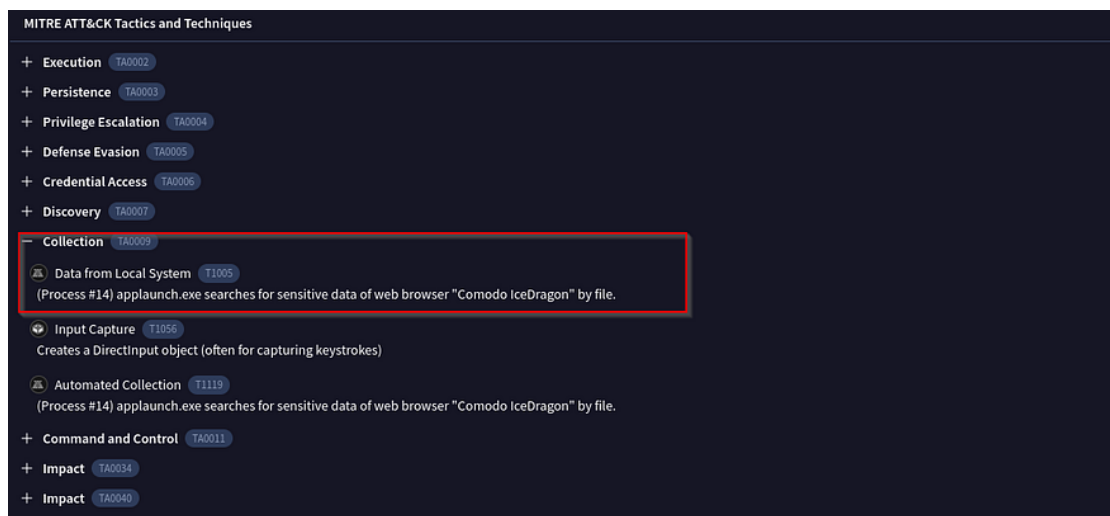
Question 3: The third question requires finding when this malware was first seen. Again, I remained on **VirusTotal**, and under the **Details** tab, I found the answer in the **History** section.

A screenshot of the VirusTotal 'History' tab. It displays a table with submission and analysis dates. The 'First Submission' row is highlighted with a red box.

Creation Time	2022-05-24 22:49:06 UTC
First Submission	2023-10-06 04:41:50 UTC
Last Submission	2024-07-18 23:57:38 UTC
Last Analysis	2024-08-10 15:49:02 UTC

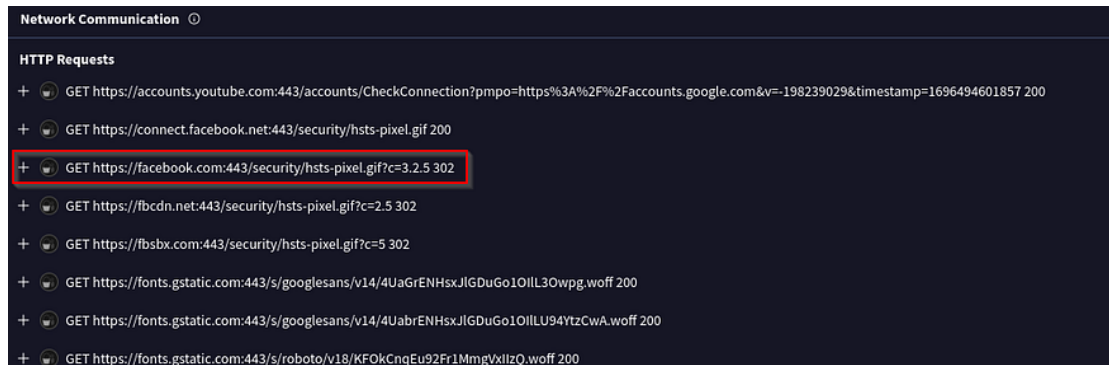
Question 3 Answer: *2023-10-06 04:41:50 UTC*

Question 4: This question involved identifying the MITRE ATT&CK technique ID for the malware's data collection before exfiltration. To find this, I moved to the **Behavior** tab on **VirusTotal** and located the relevant information under the **MITRE ATT&CK Tactics and Techniques** section.



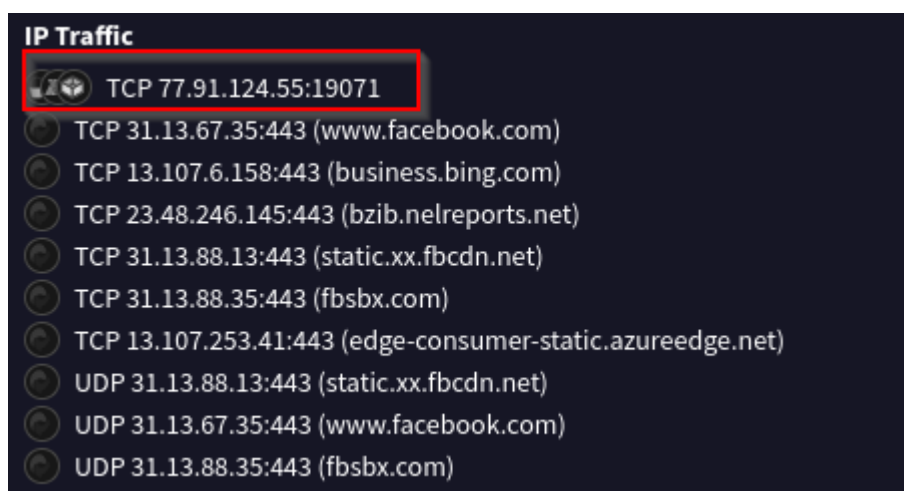
Question 4 Answer: *T1005*

Question 5: For this question, I was asked to find the domain name resolutions performed by the malware. I explored the **Behavior** tab and found the **Network Communication** section. After identifying the domains, I cross-referenced them on **VirusTotal** to check if any were flagged as malicious.



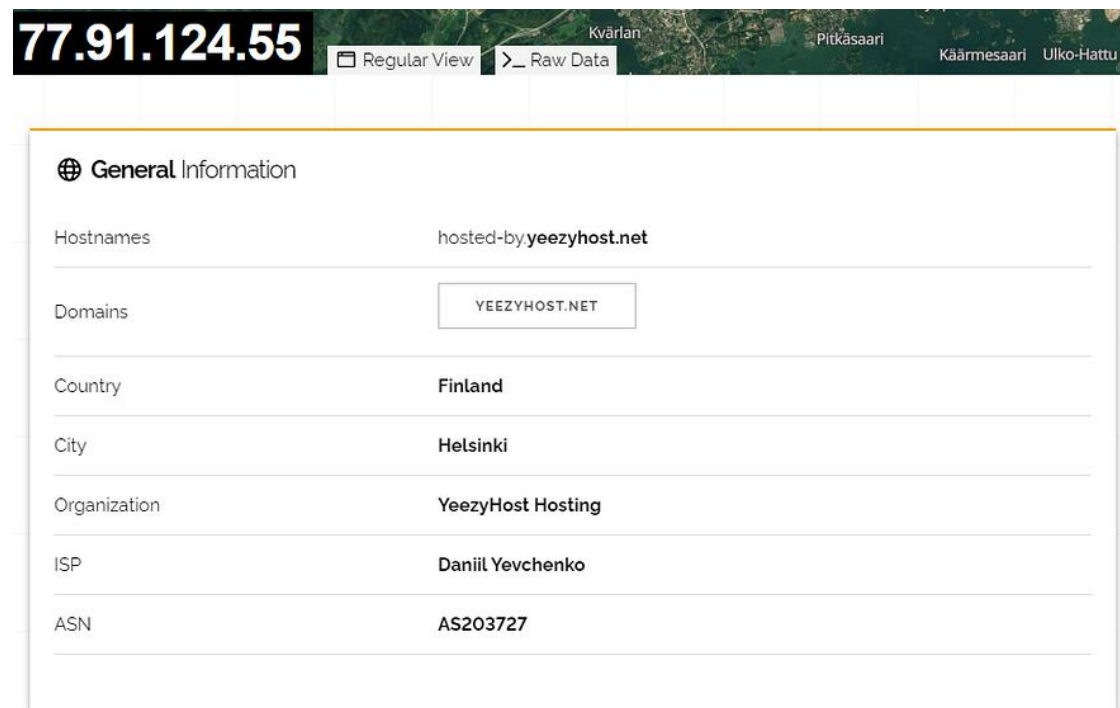
Question 5 Answer: *Facebook.com*

Question 6: This question sought the IP and Port that the malware is communicating with. I stayed in the **Behavior** tab and found the answer in the **IP Traffic** section. I further investigated the contacted IPs on **VirusTotal**, discovering that some were associated with C2 operations by malware like Amadey and Redline.



Question 6 Answer: 77.91.124.55:19071

Question 7 (This question was later removed I am keeping it here but the new question 7 is next): Originally, I was asked to find the hosting provider. I would have done this by using **Shodan** to analyze the IP. However, this question was later removed



77.91.124.55 Regular View Raw Data

General Information

Hostnames	hosted-byyeezyhost.net
Domains	YEEZYHOST.NET
Country	Finland
City	Helsinki
Organization	YeezyHost Hosting
ISP	Daniil Yevchenko
ASN	AS203727

Question 7 Answer: Yeezyhost

Question 7: This question asked me to find the YARA rule created by **Varpos** that can detect and identify the malware. To do this, I searched for the SHA-256 hash on **MalwareBazaar** and located the YARA signature in the **YARA Signatures** section.








YARA Signatures

MalwareBazaar uses YARA rules from several public and non-public repositories, such as [Malpedia](#). Those are being matched against malware samples uploaded to MalwareBazaar as well as against any suspicious process dumps they may create. Please note that only results from **TLP:WHITE** rules are being displayed.

Rule name:	detect_Redline_Stealer Alert
Author:	Varp0s
Rule name:	INDICATOR_EXE_Packed_ConfuserEx Alert
Author:	ditekSHen
Description:	Detects executables packed with ConfuserEx Mod
Rule name:	NET Alert
Author:	malware-lu

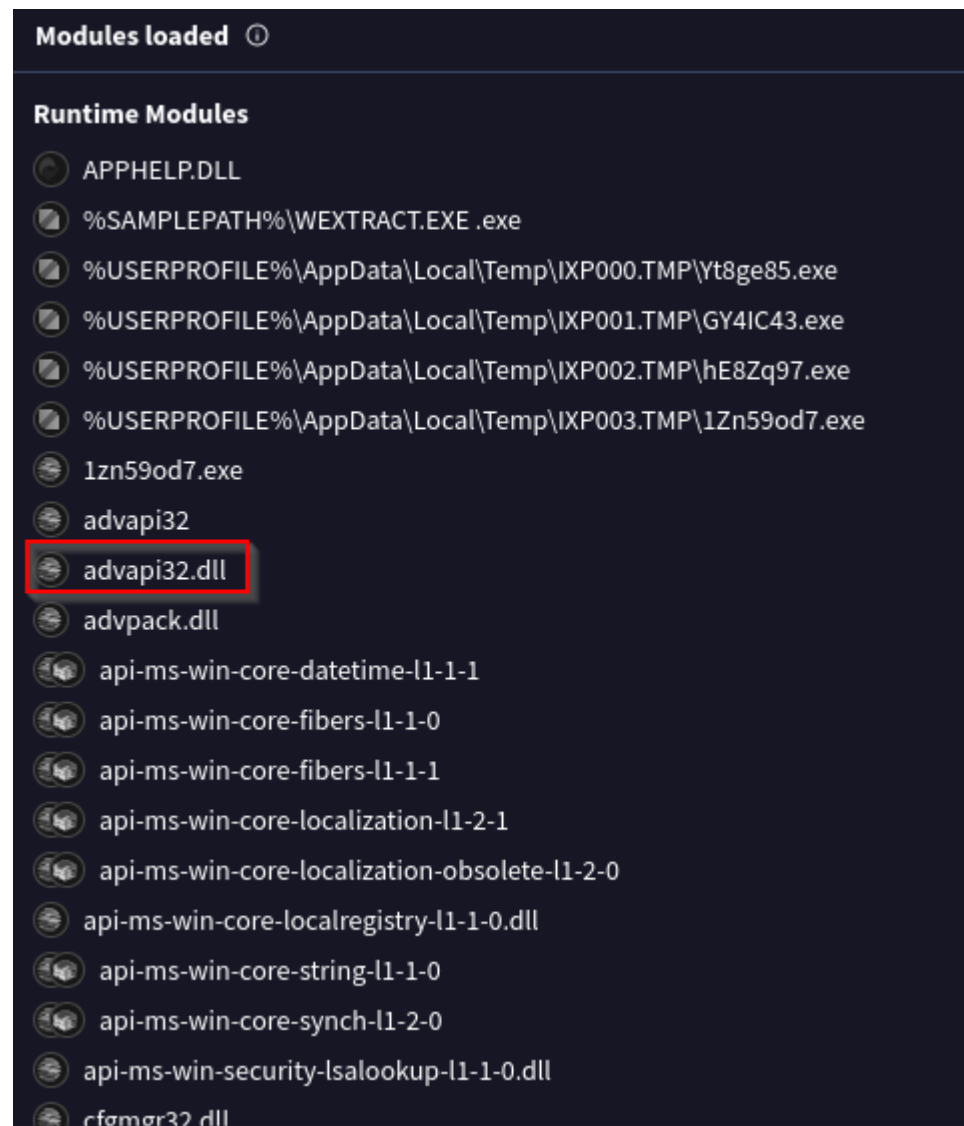
Question 7 Answer: *detect_Redline_Stealer*

Question 8: For this question, I needed to determine the alias for the malware. I utilized **ThreatFox**, searching “ioc:ip_address” and then find the section labeled **Malware Alias** to find the answer.

IOC ID:	1167880
IOC:	 77.91.124.55:19071
IOC Type @:	ip:port
Threat Type @:	botnet_cc
Malware:	 RedLine Stealer
Malware alias:	RECORDSTEALER
Confidence Level @:	 Confidence level is high (100%)
ASN:	AS701 UUNET
Country:	 US
First seen:	2023-09-27 01:05:23 UTC
Last seen:	2023-10-03 15:07:51 UTC
UUID:	efbc3ad6-5cd1-11ee-ab4a-42010aa4000a
Reporter @	 abuse_ch
Reward @	 10 credits from edwardcode
Tags:	 RedLineStealer

Question 8 Answer: *RECORDSTEALER*

Question 9: Finally, I was tasked with identifying the DLL that the malware uses for privilege escalation. I returned to **VirusTotal**, examined the **Runtime Modules** section under the **Behavior** tab, and identified several DLLs. I then researched each one to determine which was commonly used for privilege escalation, ultimately finding the correct answer.



Question 9 Answer: *advapi32.dll*

BY: Asad Dafalla