L1 SOC Report: AsyncRAT Indicators Escalation Case Study

Analyst Note:

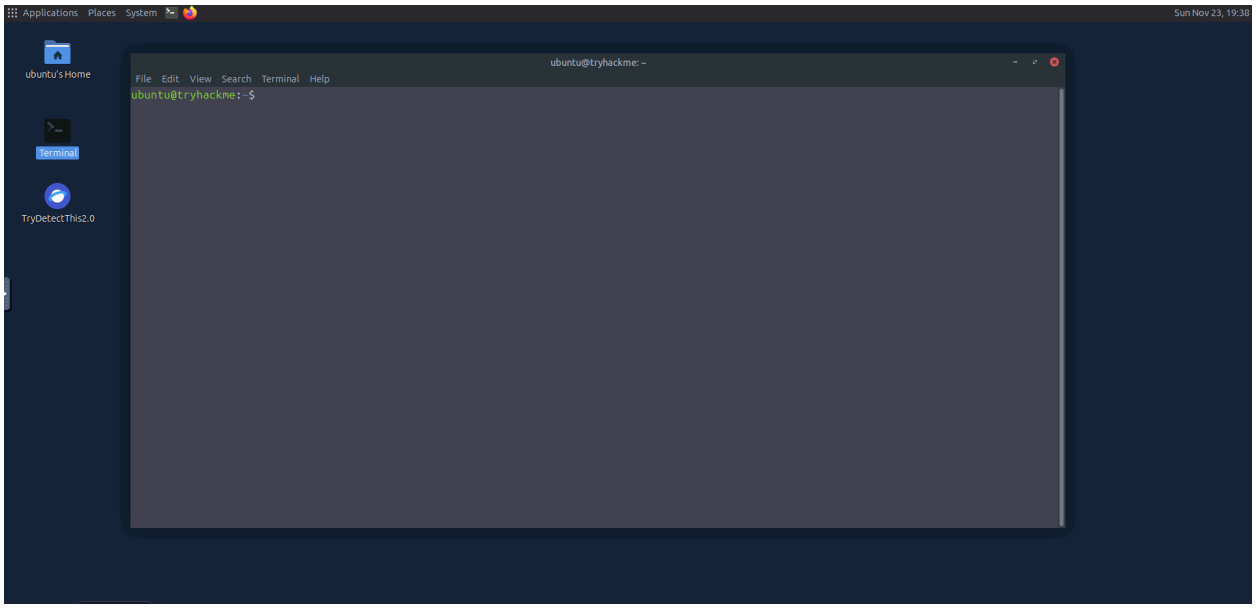
This write-up is based on an L1 investigation that was escalated to L2. As an L1 analyst, my role was to validate the threat, gather indicators, and document what I found before escalation. The deeper analysis shown in this walkthrough reflects learning practice and demonstrates my understanding of how L2 processes the malware, not actions an L1 would normally perform during live operations.

Info Provided

You are an SOC analyst on the SOC team at Managed Server Provider TrySecureMe. Today, you are supporting an L3 analyst in investigating flagged IPs, hashes, URLs, or domains as part of IR activities. One of the L1 analysts flagged two suspicious findings early in the morning and escalated them. Your task is to analyse these findings further and distil the information into usable threat intelligence.

Flagged IP: **101[.]99[.]76[.]120**
Flagged SHA256 hash:
5d0509f68a9b7c415a726be75a078180e3f02e59866f193b0a99eee8e39c874f

Lab

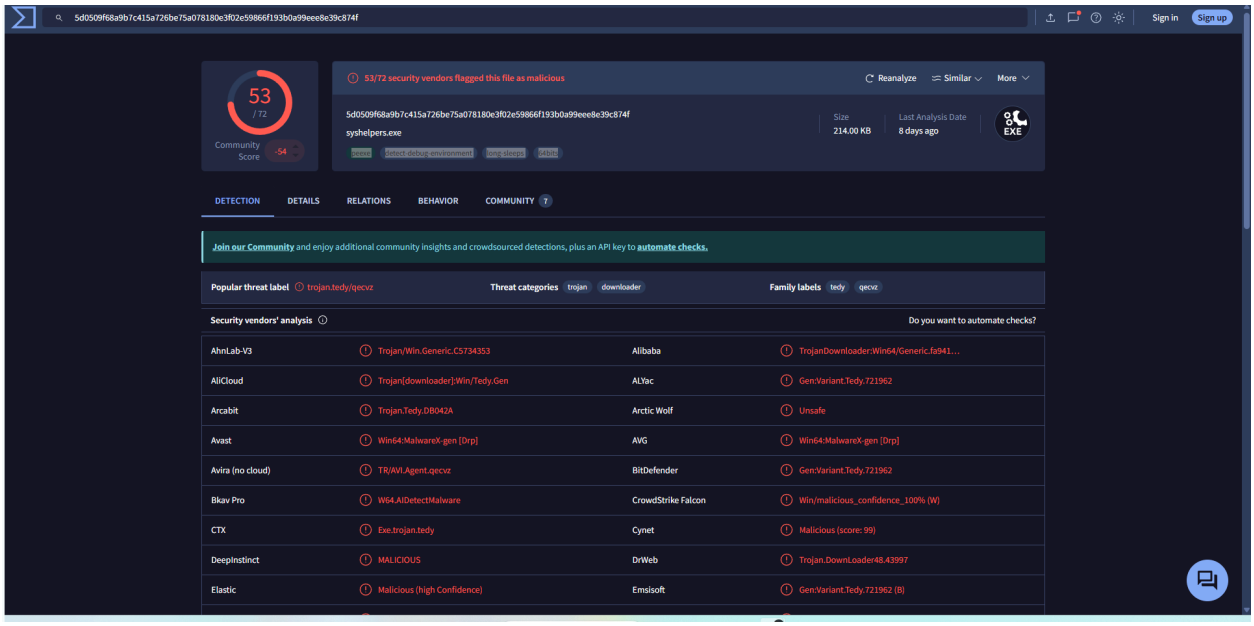


We are provided with an empty screen

Q1- What is the name of the file identified with the flagged SHA256 hash?

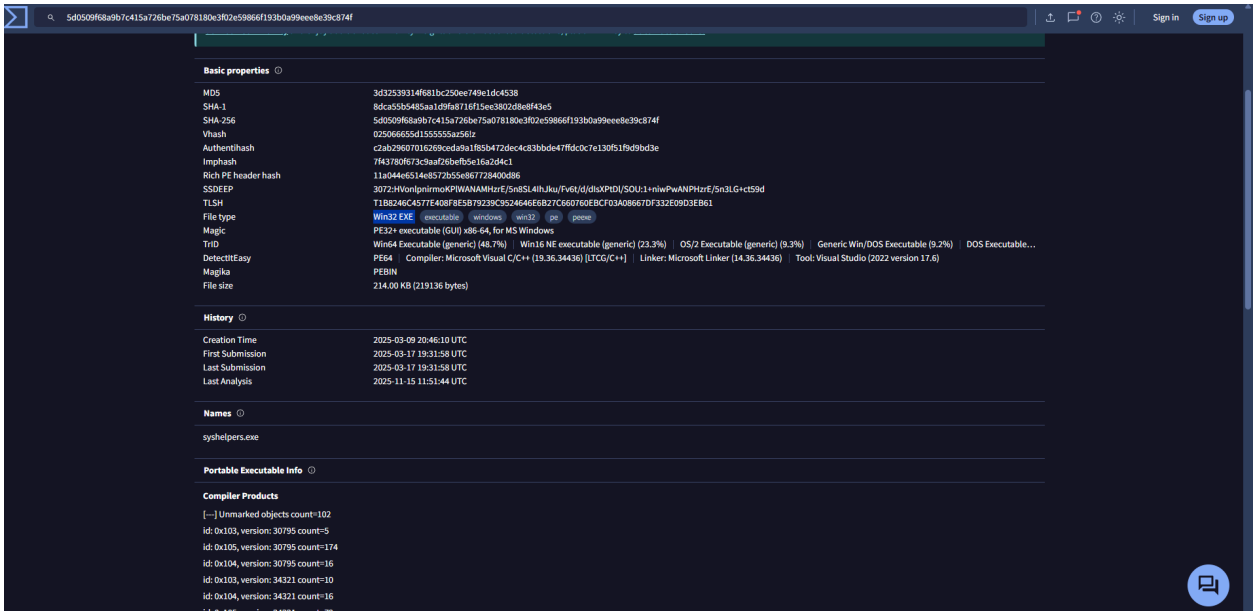
- First thing i did was check the file hash to find out more info about the file
- From VirusTotal we were able to see that this file has be flagged by 53 out of 72 vendors with the threat categories being trojan and downloader

- The tags are “ peexe, detect-debug-environment, long-sleeps, 64bits” and the File name is “syshelpers.exe”



Q2- What is the file type associated with the flagged SHA256 hash?

- After checking more about the details to learn a bit more about the file we learn that it is a Win32 EXE (executable)



Q3-What are the execution parents of the flagged hash?

- After looking at the Relations tab we find that the execution parents are :
    - 361GJX7J (SHA246-047c5eec0445746862710d20e50a5dd04510b7e625fa5c1f5d48ce078001c0de)
    - Installer.exe (SHA256-fa102d4e3cfbe85f5189da70a52c1d266925f3efd122091cdc8fe0fc39033942)

Q4- What is the name of the file being dropped?

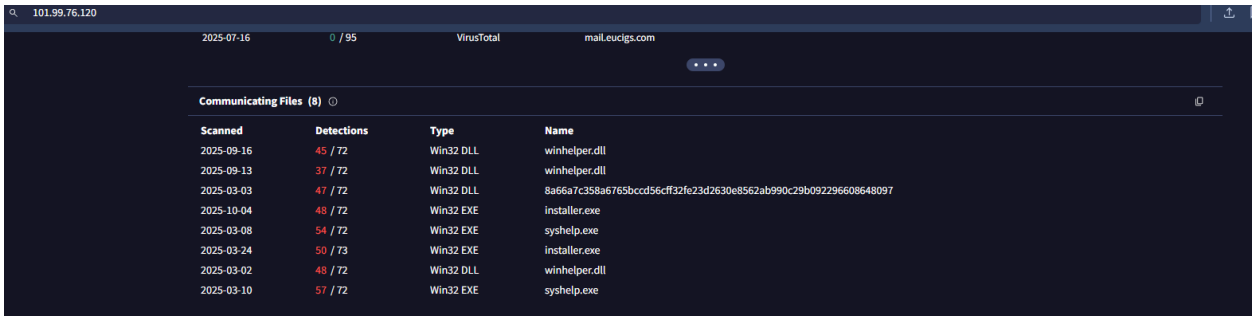
- Scrolling a little farther we see that there was one file dropped name “ AClient.exe” (SHA256-dd02c105809e4ca41a5489e585ba025eddb89a91703b73a566c9903e6406a08c)

Q5- Research the second hash in question 3 and list the four malicious dropped files in the order they appear (from up to down), separated by commas.

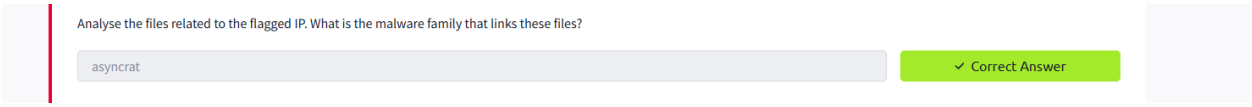
- After looking into the second file “Installer.exe” we see that the 4 malicious dropped files from below

Q6- Analyse the files related to the flagged IP. What is the malware family that links these files?

- Now its time to look into the suspicious IP. After typing the IP address into VirusTotal we see that the ip has been flagged from 9 different vendors indicating that theres some suspicious activity going on.
- To answer this question you have to look into the communicating files section under the relations tab to see all the files related to the IP.

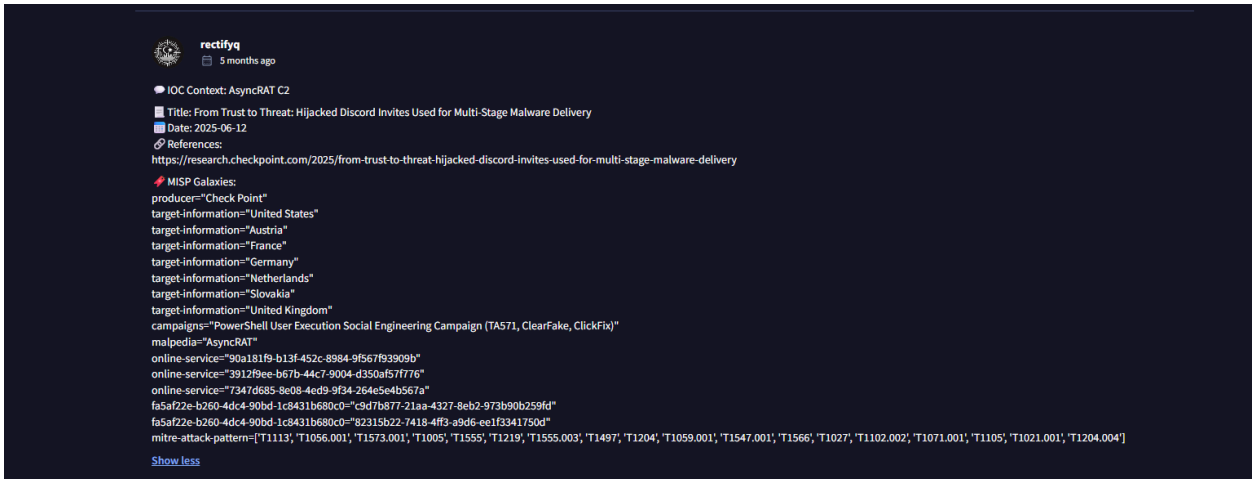


- After clicking through each one we can see that they have a common tag of “asyncrat” in the family tags section.
- We then learn AsyncRAT is a popular malware family used by a range of threat actors to target Windows systems.They are a type of malware that enables attackers to remotely control infected computers.



Q7- What is the title of the original report where these flagged indicators are mentioned?

- This question is kind of confusing as its really vauge and even when you search the answer its hidden in different titled blogs
- Checking the community tab though you see this post containing a blog from Checkpoint giving us the answer to the question



Q8- Which tool did the attackers use to steal cookies from the Google Chrome browser?

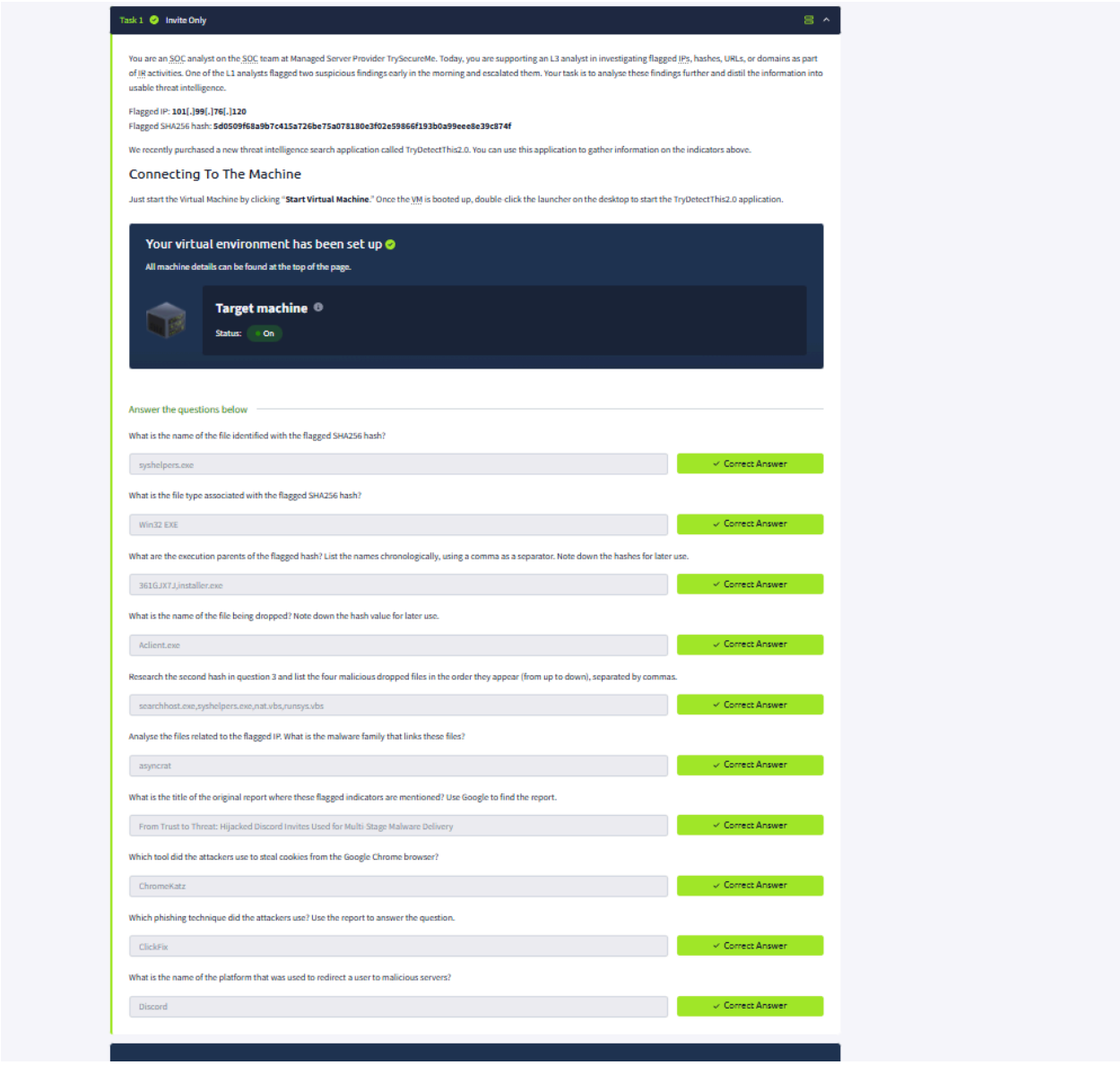
Q9- Which phishing technique did the attackers use? Use the report to answer the question.

Q10- What is the name of the platform that was used to redirect a user to malicious servers?

- Im going to pair the last three questions together because you learn them from reading the article we found.
- From the key takeaways we learn that
  - Check Point Research uncovered an active malware campaign exploiting expired and released Discord invite links. Attackers

hijacked the links through vanity link registration, allowing them to silently redirect users from trusted sources to malicious servers.
    - The attackers combined the ClickFix phishing technique, multi-stage loaders, and time-based evasions to stealthily deliver AsyncRAT, and a customized Skuld Stealer targeting crypto wallets.
    - Payload delivery and data exfiltration occur exclusively via trusted cloud services such as GitHub, Bitbucket, Pastebin, and Discord, helping the operation blend into normal traffic and avoid raising alarms.
    - The operation continues to evolve, and threat actors can now bypass Chrome's App Bound Encryption (ABE) by using adapted tools like ChromeKatz to steal cookies from new Chromium browser versions.

And thats the end of the lab completed



Escalation Summary (L1 Role):

After confirming the indicators were malicious and linked to an AsyncRAT campaign, I would escalate the case to the L2 analyst with all gathered IOCs, screenshots, and notes. Any containment, eradication, or deeper malware analysis would be handled by L2/L3. My walkthrough above reflects the extended analysis I performed for training and portfolio

purposes.