

# 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

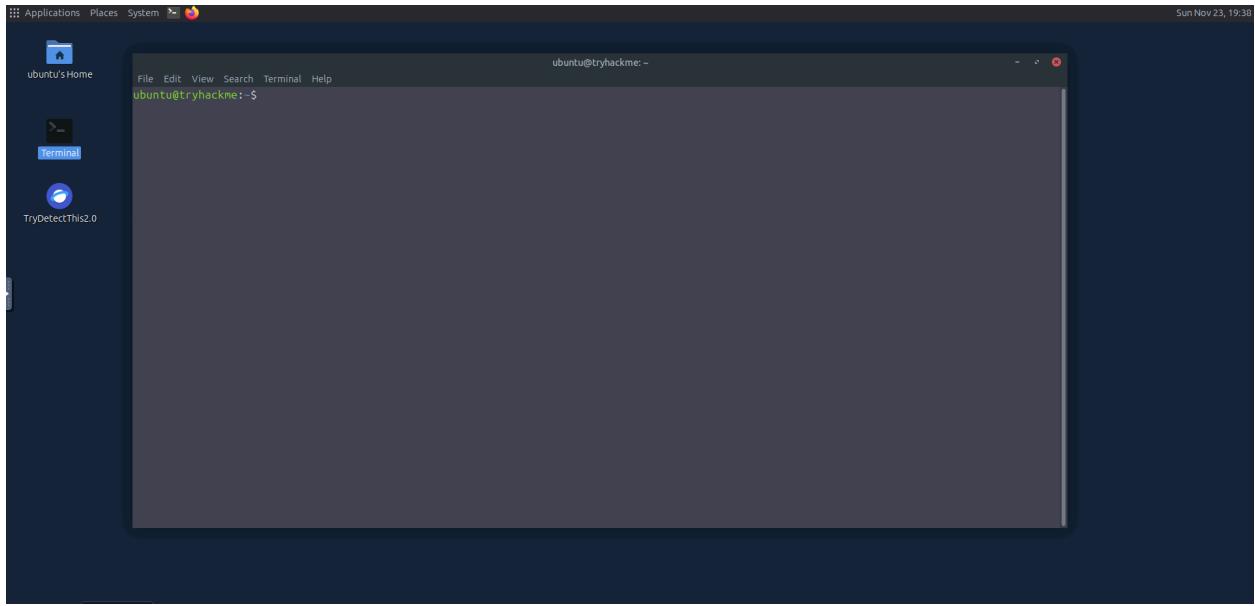
You are an SOC analyst on the SOC team at Managed Server Provider TrySecureMe. Today, you are supporting an L3 analyst in investigating flagged IPs, hashes, URLs, or domains as part of IR activities. One of the L1 analysts flagged two suspicious findings early in the morning and escalated them. Your 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 been 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”

Security vendor's analysis		Do you want to automate checks?	
AhnLab-V3	Trojan/Win.Generic.C.5734333	AliBaba	TrojanDownloader:Win64/Generic.fa941...
AllCloud	Trojan[downloader]:Win/Tedy.Gen	ALYac	Gen.Variant.Tedy.721962
Arcabit	Trojan.Tedy.DB042A	Arctic Wolf	Unsafe
Avast	Win64:MalwareX.gen [Dlp]	AVG	Win64:MalwareX.gen [Dlp]
Avira (no cloud)	TR/AVLAgent.qecvz	BitDefender	Gen.Variant.Tedy.721962
Blav Pro	W64:ADetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Eve.trojan.tedy	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	Trojan.DownLoader:48.43997
Elastic	Malicious (high Confidence)	Emsisoft	Gen.Variant.Tedy.721962 (B)

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)

Basic properties	
MD5	3d12539314f681bc250ee749e1dc4538
SHA-1	8dc5a5545485a1dfa71f1f5ee38028ef43e5
SHA-256	5d0509f68a9b7c415a726be75a078180e3f02e59866f193ba099ee8e39c874f
Vhash	02506655155555aa5e5612
Authentihash	c2ab29607016269cededa9a185b472de4c433b8de47ffcc07e7e130f51f9d9bd3e
ImpHash	7f43780f673c3aaaf76bf5b5e16a2d4c1
Rich PE header hash	11a044e6514e5725b5e897728400b6
SSDEEP	3072:W0n!pnjmr0KPNWANAMHzr/5n8SL4HJu/Fw6/dlxXPxD/SOU1+nwPwNPnIrZ/5n3LG+cct59d
TLS1	T1B8246C4577E408F8E5B79239C95246466B277C660760EBCE03A08667DF332E09D3EB61
File type	Win32 EXE executable windows win32 pe pexe
Magic	PE32+ executable (GU) x86-64, for MS Windows
TrID	Win64 Executable (generic) (48.7%) Win16 NE executable (generic) (23.3%) OS/2 Executable (generic) (9.3%) Generic Win/DOS Executable (9.2%) DOS Executable...
DetectEasy	P64 Compiler: Microsoft Visual C/C++ (19.36.34436) [ITCG/C++] Linker: Microsoft Linker (14.36.34436) Tool: Visual Studio (2022 version 17.6)
Magika	PEBIN
File size	214.00 KB (219136 bytes)

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 )

Execution Parents (2)			
Scanned	Detections	Type	Name
2025-05-08	15 / 62	Powershell	361GJX7J
2025-11-19	35 / 72	Win32 EXE	installer.exe

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)

Dropped Files (1)			
Scanned	Detections	File type	Name
2025-09-14	0 / 62	?	AClient.exe

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

Scanned	Detections	File type	Name
2025-03-17	37 / 73	Win32 EXE	searchHost.exe
2025-11-15	53 / 72	Win32 EXE	syshelpers.exe
2025-02-28	1 / 60	VBA	nat1.xlsb
2024-09-13	0 / 64	Text	tavspvru.cs
2025-09-27	0 / 64	PDF	bitaddress.pdf
2025-11-23	0 / 60	PowerShell	_PSScriptPolicyTest_zq5bcsr0.ohk.ps1
2025-03-17	0 / 73	Win32 DLL	gcsnnmn.dll
2025-06-26	2 / 62	VBA	runsys.xlsb
2024-09-16	0 / 65	ZIP	browsers.zip
2025-03-17	0 / 65	ZIP	commonfiles.zip

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.

Scanned	Detections	Type	Name
2025-09-16	45 / 72	Win32 DLL	winhelper.dll
2025-09-13	37 / 72	Win32 DLL	winhelper.dll
2025-03-03	47 / 72	Win32 DLL	8a66a7c35ba6765bccd56cff3fe23d2630e8562ab990c29b092296608648097
2025-10-04	48 / 72	Win32 EXE	installer.exe
2025-03-08	54 / 72	Win32 EXE	syshelp.exe
2025-03-24	50 / 73	Win32 EXE	installer.exe
2025-03-02	48 / 72	Win32 DLL	winhelper.dll
2025-03-10	57 / 72	Win32 EXE	syshelp.exe

- 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.

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

asyncrat

✓ Correct Answer

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

- This question is kind of confusing as its really vague 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

The screenshot shows a social media post from a user named 'rectifyq'. The post includes a profile picture of a person with glasses, the name 'rectifyq', and a timestamp '5 months ago'. Below the post, there is a link to an IOC Context: AsyncRAT C2 report. The report details a campaign titled 'From Trust to Threat: Hijacked Discord Invites Used for Multi-Stage Malware Delivery' dated 2025-06-12. It provides a reference URL: <https://research.checkpoint.com/2025/from-trust-to-threat-hijacked-discord-invites-used-for-multi-stage-malware-delivery>. The report also lists various MISP Galaxies and associated IOC data.

IOC Context: AsyncRAT C2  
Title: From Trust to Threat: Hijacked Discord Invites Used for Multi-Stage Malware Delivery  
Date: 2025-06-12  
References:  
<https://research.checkpoint.com/2025/from-trust-to-threat-hijacked-discord-invites-used-for-multi-stage-malware-delivery>  
MISP Galaxies:  
producer="Check Point"  
target-information="United States"  
target-information="Austria"  
target-information="France"  
target-information="Germany"  
target-information="Netherlands"  
target-information="Slovakia"  
target-information="United Kingdom"  
campaigns="PowerShell User Execution Social Engineering Campaign (TA571, ClearFake, ClickFix)"  
malpedia="AsyncRAT"  
online-service="90a181fb-b13f-452c-8984-9f5e7fb3909b"  
online-service="3912f9ee-b67b-44c7-9004-d350af57ff76"  
online-service="7347d685-8e08-4ed9-9f34-264e5e4d0567a"  
fa5a722e-b260-4dc4-90bd-1c8431b680c0="c9db7b87-21aa-4327-8eb2-973b90b259fd"  
fa5a722e-b260-4dc4-90bd-1c8431b680c0="8231522-7418-4f3-9d6-e1f3341750d"  
mitre-attack-pattern=[T1113', 'T1056.001', 'T1573.001', 'T1005', 'T1555', 'T1219', 'T1555.003', 'T1497', 'T1204', 'T1059.001', 'T1547.001', 'T1566', 'T1027', 'T1102.002', 'T1071.001', 'T1105', 'T1021.001', 'T1204.004']  
Show less

## 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?

- I'm 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 that's the end of the lab completed

Task 1. Invite Only

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 distill the information into usable threat intelligence.

Flagged IP: 101.199.176.120  
Flagged SHA256 hash: 5d0509f68a9b7c415a726be75a078180e3f02e59866f193b0a99eee8e39c874f

We recently purchased a new threat intelligence search application called TryDetectThis2.0. You can use this application to gather information on the indicators above.

**Connecting To The Machine**

Just start the Virtual Machine by clicking "Start Virtual Machine." Once the VM is booted up, double-click the launcher on the desktop to start the TryDetectThis2.0 application.

**Your virtual environment has been set up**   
All machine details can be found at the top of the page.

**Target machine**   
Status: On

Answer the questions below

What is the name of the file identified with the flagged SHA256 hash?  
 Correct Answer

What is the file type associated with the flagged SHA256 hash?  
 Correct Answer

What are the execution parents of the flagged hash? List the names chronologically, using a comma as a separator. Note down the hashes for later use.  
 Correct Answer

What is the name of the file being dropped? Note down the hash value for later use.  
 Correct Answer

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.  
 Correct Answer

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

What is the title of the original report where these flagged indicators are mentioned? Use Google to find the report.  
 Correct Answer

Which tool did the attackers use to steal cookies from the Google Chrome browser?  
 Correct Answer

Which phishing technique did the attackers use? Use the report to answer the question.  
 Correct Answer

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

## 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.*