

# 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

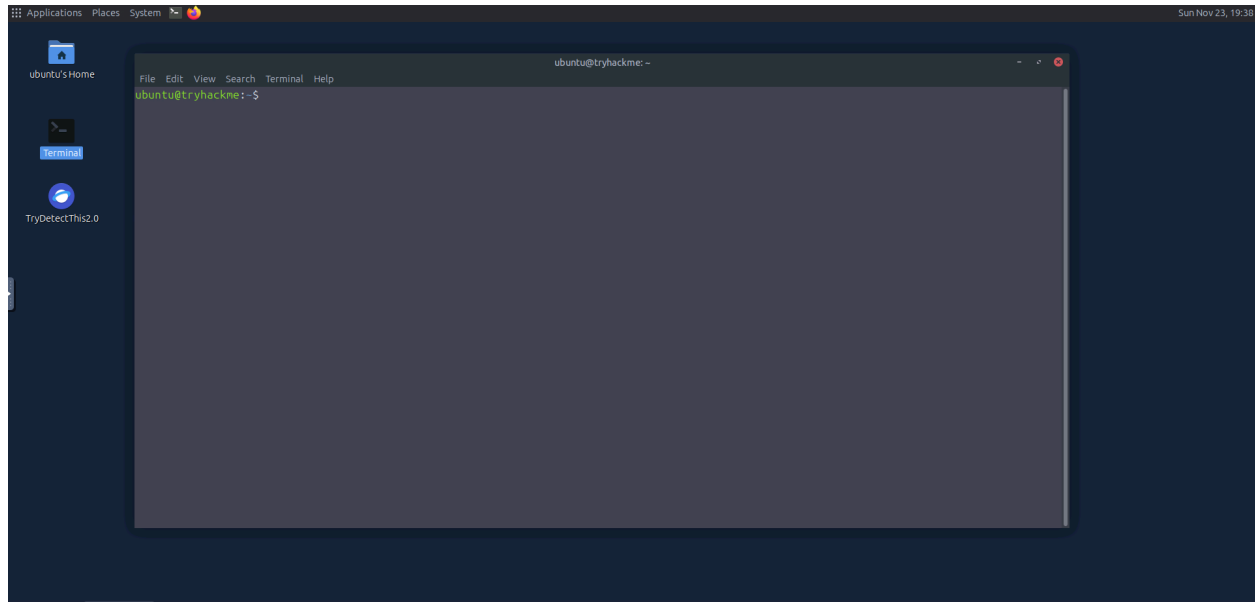
You are an SOC analyst on the SOC team at Managed Server Provider TrySecureMe. Today, you are supporting an L3 analyst in investigating flagged IPs, hashes, URLs, or domains as part of IR activities. One of the L1 analysts flagged two suspicious findings early in the morning and escalated them. Your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

- 53

/ 72

Community Score

-54

53/72 security vendors flagged this file as malicious

Reanalyze

Similar

More

S50509f68a9b7c415a726be75a078180c3f02e5986f193b0a99ee0e39c874f

Size

214.0 KB

Last Analysis Date

8 days ago

EXE

systelpers.exe

View

threat details

threat checks

public

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Join our Community

and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label

trojan.tedy.qecvz

Threat categories

trojan

downloader

Family labels

tedy

qecvz

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Trojan.Win.Generic.C5734353	Alibaba	TrojanDownloader.Win64/Generic.faf41...
AliCloud	Trojan(downloader).Win/Tedy.Gen	ALYac	Gen.Variant.Tedy.721962
ArcaBit	Trojan.Tedy.D8042A	Arctic Wolf	Unsafe
Avast	Win64-MalwareX-gen [Drp]	AVG	Win64-MalwareX-gen [Drp]
Avira (no cloud)	TR/ML.Agent.qecvz	BitDefender	Gen.Variant.Tedy.721962
Bkav Pro	W64.AI.Detect.Malware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.tedy	Cynet	Malicious (score: 99)
DeepInSight	MALICIOUS	DrWeb	Trojan.Down.Loader48.43997
Elastic	Malicious (High Confidence)	Emsisoft	Gen.Variant.Tedy.721962 (B)

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

Q

Sd0509f8a9b7c415a726be75a078180bc302e59866f193b0a99eeec839c87af

🔍 🗄️ ⚙️ 🔒

Sign In Sign Up

Basic properties

MDS	3432530314f681bc250ec749e1dc4538
SHA-1	8dca55b5485aa1d9fa8716f1Sec3802d8ef43e5
SHA-256	Sd0509f8a9b7c415a726be75a078180bc302e59866f193b0a99eeec839c87af
Vhash	c25066655d1555555asr56lz
AuthenticHash	02ab29607D16269cedafa180b472dec4c83bbde47fdcc7e130F51f9d9bd3e
ImpHash	F43B80ff67fc3aaf2feeb0e15a204c1
Rich PE header hash	11a04ae5314e87285e687726a0d86
SSDEP	3072+VnlglnrmKPWAMNHxzf/fs0S4LHJku/Fvt/d/shoPDI/SOU:1+nhePeANPHzrf/SoLLG+cst9d
TLSH	T1B8246C457FE408F8E5879239C9524646E6B27C660760BCF03A08667DF332ED9D3EB61
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32+ executable (GUI) 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...
DetectItEasy	PE#4 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)

History

Creation Time	2025-03-09 20:46:10 UTC
First Submission	2025-03-17 19:31:58 UTC
Last Submission	2025-03-17 19:31:58 UTC
Last Analysis	2025-11-15 11:51:44 UTC

Names

sylshelpers.exe

Portable Executable Info

Compiler Products  
[—] Unmarked objects count=102  
id: 0x103, version: 30795 count=5  
id: 0x105, version: 30795 count=174  
id: 0x104, version: 30795 count=16  
id: 0x103, version: 34321 count=10  
id: 0x104, version: 34321 count=16

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

fa102d4e3cbe85f5189da70a52c1d266925f3ef122091cdc8e0fc39033942

Scanned	Detections	File type	Name
2025-11-09	0 / 62	ICO	18.ico
2022-06-08	0 / 96	ICO	108
2025-11-10	0 / 62	ICO	11.ico
2025-11-10	0 / 62	ICO	12.ico

**Dropped Files (32)**

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.vbs
2024-09-13	0 / 64	Text	taxwpSru.0.cs
2025-09-27	0 / 64	PDF	bitaddress.pdf
2025-11-23	0 / 60	Powershell	__PSScriptPolicyTest_req5bcurt.ohk.psm1
2025-03-17	0 / 73	Win32 DLL	gconn1nn.dll
2025-06-26	2 / 62	VBA	runsys.vbs
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.

101.99.76.120

2025-07-16 0 / 95 VirusTotal mail.eucigs.com

**Communicating Files (8)**

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	8a66a7c358a6765bccd56cf32fe23d2630e8562ab990c29b092296608648097
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 “asynrat” 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?

asynccrat

✓ 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 blog post from Check Point Research. The title is "From Trust to Threat: Hijacked Discord Invites Used for Multi-Stage Malware Delivery". The date is 2025-06-12. The post includes a reference to a research report and a list of indicators of compromise (IOCs) such as IP addresses, domain names, and file hashes. The IOCs are listed under the heading "MISP Galaxies".

**IOCs 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="90a181f9-b13f-452c-8984-9f567f93909b"  
online-service="3912f9ee-b67b-44c7-9004-d350af571776"  
online-service="7347d685-8e08-4ed9-9f34-264e5e4b567a"  
fa5af22e-b260-4dc4-90bd-1c8431b680c0="c9d7b877-21aa-4327-8eb2-973b90b259fd"  
fa5af22e-b260-4dc4-90bd-1c8431b680c0="82315b22-7418-4ff3-a9d6-eef3341750d"  
mitre-attack-pattern=["T1113", "T1096.001", "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?

- 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

Task 1 Invite Only

You are an SOC analyst on the SOC team at Managed Server Provider TrySecureMe. Today, you are supporting an L1 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: 5d0509f68a9b7c415a726be75a078180e3f02e59866f193ba99ee8e39c874f

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 <sup>®</sup>

Status: On

Answer the questions below

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

tyshelpers.exe ✓ Correct Answer

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

Win32 EXE ✓ 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.

361GJXTJninstaller.exe ✓ Correct Answer

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

hclient.exe ✓ 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.

searchhost.exe,tyshelpers.exe,nat.vbs,runsys.vbs ✓ Correct Answer

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

asynicrat ✓ Correct Answer

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

From Trust to Threat: Hijacked Discord Invites Used for Multi-Stage Malware Delivery ✓ Correct Answer

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

ChromeKatz ✓ Correct Answer

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

ClickFix ✓ Correct Answer

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

Discord ✓ 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.*