

Friday Overtime CTF

The artifacts in this scenario originate from an actual cyber-attack. For safety reasons, it is strongly recommended to interact with them only within the provided virtual machine (VM), which operates in a secure, isolated environment. This is a subscription only for TryHackMe users. It was created by TryHackMe. Here is the link to the project room TryHackMe Room — Friday Overtime. (<https://tryhackme.com/room/fridayovertime>)


Hello Busy Weekend. . .

It's a Friday evening at PandaProbe Intelligence when a notification appears on your CTI platform. While most are already looking forward to the weekend, you realise you must pull overtime because SwiftSpend Finance has opened a new ticket, raising concerns about potential malware threats. The finance company, known for its meticulous security measures, stumbled upon something suspicious and wanted immediate expert analysis. As the only remaining CTI Analyst on shift at PandaProbe Intelligence, you quickly took charge of the situation, realising the gravity of a potential breach at a financial institution. The ticket contained multiple file attachments, presumed to be malware samples. With a deep breath, a focused mind, and the longing desire to go home, you began the process of:

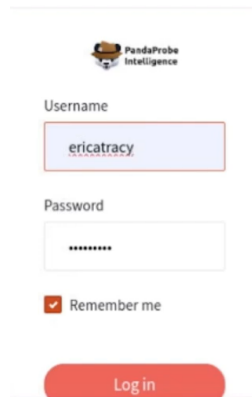
1. Downloading the malware samples provided in the ticket, ensuring they were contained in a secure environment.
2. Running the samples through preliminary automated malware analysis tools to get a quick overview.
3. Deep diving into a manual analysis, understanding the malware's behaviour, and identifying its communication patterns.
4. Correlating findings with global threat intelligence databases to identify known signatures or behaviours.
5. Compiling a comprehensive report with mitigation and recovery steps, ensuring SwiftSpend Finance could swiftly address potential threats.

Connecting to the machine

Start the virtual machine by clicking the green **Start Machine** button on the upper right section of this task. If the VM is not visible, use the blue **Show Split View** button at the top-right of the page. Additionally, you can open the DocIntel platform using the credentials below.



Username	ericatracy
Password	Intel321!
IP	MACHINE_IP



PandaProbe Intelligence

Username

ericatracy

Password

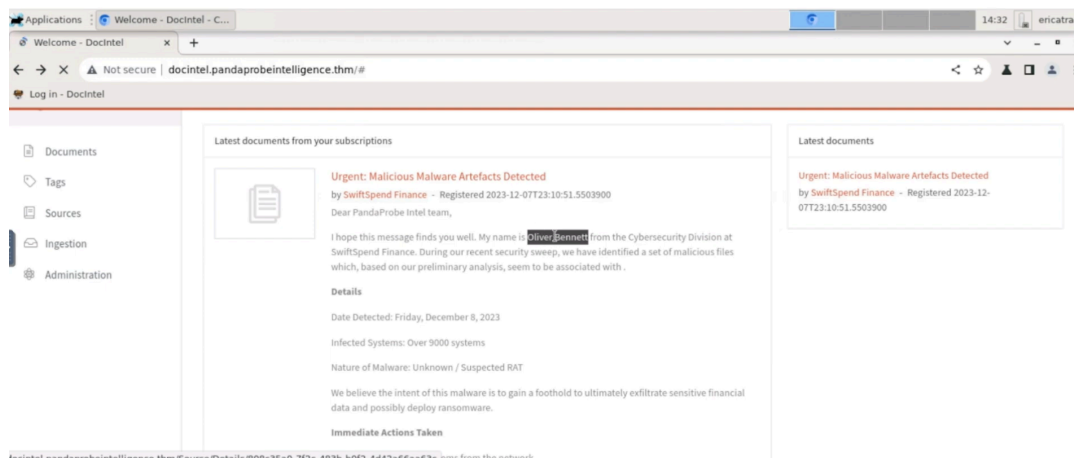
☒ Remember me

Log in

Note: While the web browser (i.e., Chromium) will immediately start after boot up, it may show a tab that has a "502 Bad Gateway" error message displayed. This is because the DocIntel platform takes about 5 more minutes to finish starting up after the VM has completely booted up. After 5 minutes, you can refresh the page in order to view the login page. We appreciate your patience. The ticket details can be found by logging in to the DocIntel platform. OSINT, a web browser, and a text editor outside the VM will also help.

Answer the questions below

Who shared the malware samples?



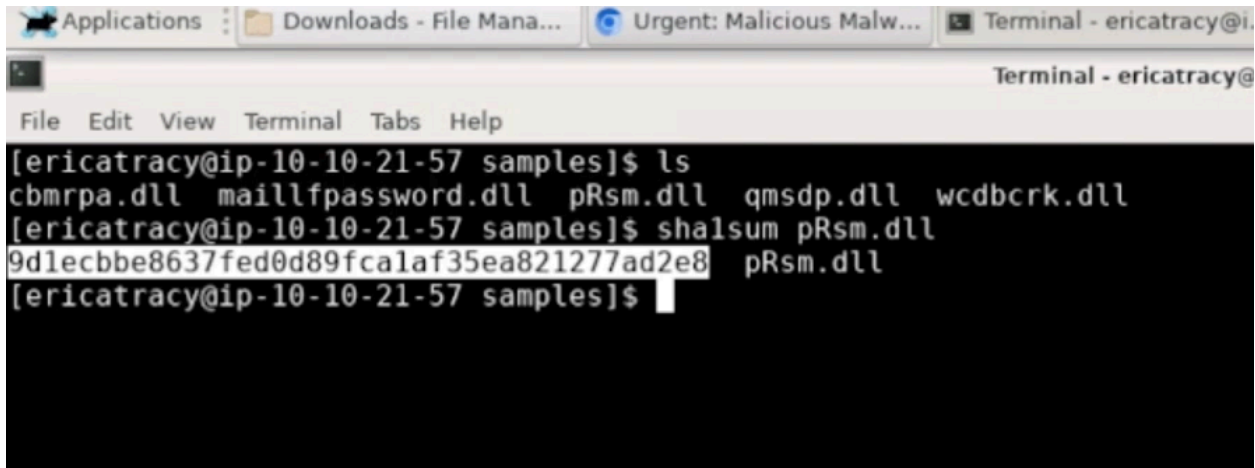
After logging into the DocIntel platform, you'll see the latest documents from your subscriptions displayed. Begin reviewing the emails/documents, and you should be able to quickly identify the sender's name.

Answer : Oliver Bennett

What is the SHA1 hash of the file “pRsm.dll” inside samples.zip?

To start extracting the contents of samples.zip, use the command `unzip samples.zip`. However, before proceeding, you'll need the password provided in the previous section, which is “Panda321!”. Enter this password when prompted and press Enter — the files will then be extracted to the current directory.

For the SHA1 hash of the file, we will use the command `sha1sum pRsm.dll`. Pressing enter will run the command and show the SHA1 hash.

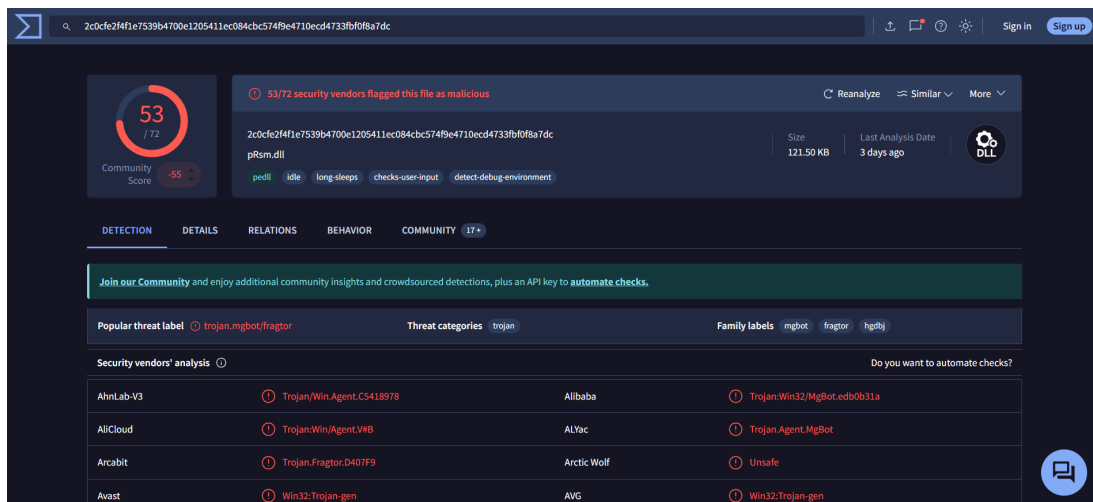


```
[ericatracy@ip-10-10-21-57 samples]$ ls
cbmrpa.dll  maillfpassword.dll  pRsm.dll  qmsdp.dll  wcdbrck.dll
[ericatracy@ip-10-10-21-57 samples]$ sha1sum pRsm.dll
9d1ecbbe8637fed0d89fca1af35ea821277ad2e8  pRsm.dll
[ericatracy@ip-10-10-21-57 samples]$
```

Answer : 9d1ecbbe8637fed0d89fca1af35ea821277ad2e8

Which malware framework utilizes these DLLs as add-on modules?

To find the answer to this question, we can search this file by OSINT techniques.



The screenshot shows the VirusTotal analysis page for the file `pRsm.dll` (SHA1: 9d1ecbbe8637fed0d89fca1af35ea821277ad2e8). The file is 121.50 KB and was last analyzed 3 days ago. It has a Community Score of 53/72, with 53/72 security vendors flagging it as malicious. The file is categorized as a Trojan, specifically a Trojan.MgBot.Fragtor. The analysis shows that the file is a DLL and contains several suspicious behaviors, including long sleeps, checks for user input, and detection of debug environments. The security vendors' analysis table shows that the file is detected as a Trojan by AhnLab-V3, AliCloud, Arcabit, Avast, Alibaba, ALYac, Arctic Wolf, AVG, and others.

Security vendors' analysis	Do you want to automate checks?
AhnLab-V3	Trojan.Win.Agent.C5418978
Alibaba	Trojan.Win32/MgBot.edb0b31a
AliCloud	Trojan.Win.Agent.VWB
ALYac	Trojan.Agent.MgBot
Arcabit	Trojan.Fragtor.D407F9
Arctic Wolf	Unsafe
Avast	Win32:Trojan-gen
AVG	Win32:Trojan-gen

DLLs (Dynamic Link Libraries) are often used as modular components that extend the core functionality of the malware. Or we can find it by using search engines like google.

welivesecurity by **ESET** | Award-winning news, views, and insight from the ESET security community | English

TIPS & ADVICE | BUSINESS SECURITY | ESET RESEARCH | **WeLiveScience** | FEATURED | TOPICS | ABOUT US

Panda, where update channels of legitimate applications were mysteriously hijacked to deliver the installer for the MgBot malware, Evasive Panda's flagship backdoor.

Key points of the report:

- Users in mainland China were targeted with malware delivered through updates for software developed by Chinese companies.
- We analyze the competing hypotheses of how the malware could have been delivered to targeted users.
- With high confidence we attribute this activity to the Evasive Panda APT group.
- We provide an overview of Evasive Panda's signature backdoor MgBot and its toolkit of plugin modules.

Table of Contents

- Evasive Panda profile
- Campaign overview
- Attribution
- Technical analysis
- Conclusion
- IoCs
- MITRE ATT&CK techniques

Answer : MgBot

Which MITRE ATT&CK Technique is linked to using pRsm.dll in this malware framework?

MgBot's modular design enables it to enhance its capabilities by downloading and executing additional modules on the infected system. Search the related pRsm.dll to find the answer.

defined a minimum and maximum size.

Cbmrpa.dll	Captures text copied to the clipboard and logs information from the USBSTOR registry key.
pRsm.dll	Captures input and output audio streams.
	Credential stealer.
mailLFPassword.dll	Steals credentials from Outlook and Foxmail email client software.
	Credential stealer.

T1560.002	Archive Collected Data: Archive via Library	MgBot's plugin module <code>sebasek.dll</code> uses <code>aPLib</code> to compress files staged for exfiltration.
T1123	Audio Capture	MgBot's plugin module <code>pRsm.dll</code> captures input and output audio streams.
T1119	Automated Collection	MgBot's plugin modules capture data from various sources.

Answer : T1123 (Audio Capture)

What is the CyberChef defanged URL of the malicious download location first seen on 2020-11-02?

Find the first URL download seen by search the download information.

Table 1. Malicious **down**load locations according to ESET telemetry

URL	First seen	Domain IP
		123.151.72[.]7
<code>http://update.browser.qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe</code>	2020-11-02	
		183.232.96[.]1
		61.129.7[.]35

Input

http://update.browser.qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe

ABC 61

1

Output

hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe

Use cyberchef to get the defanged url.

Answer : `hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe`

What is the CyberChef defanged IP address of the C&C server first detected on 2020-09-14 using these modules?

Use the similar process on the previous step. But, try to find the IP address on the information table.

Network

IP	Provider	First seen	Details
122.10.88[.]226	AS55933 Cloudie Limited	2020-07-09	MgBot C&C server.
122.10.90[.]12	AS55933 Cloudie Limited	2020-09-14	MgBot C&C server.

Input

122.10.90.12

abc 12 1 12

Output

122[.]10[.]90[.]12

Make sure that we delete the square bracket when we input the IP address in cyberchef.

Answer : 122[.]10[.]90[.]12

What is the md5 hash of the spyagent family spyware hosted on the same IP targeting Android devices in June 2025?

Search using the same defanged IP address and find on the relations section.

122.10.90.12

DETECTION

DETAILS

RELATIONS

COMMUNITY 10

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

Passive DNS Replication (1)

Date resolved	Detections	Resolver	Domain
2023-04-26	2 / 94	VirusTotal	feiyuxiao01.oicp.net

Communicating Files (4)

Scanned	Detections	Type	Name
2025-03-13	60 / 73	Win32 EXE	flashplayerax_install.exe
2025-01-22	54 / 71	Win32 EXE	ald_j.exe
2024-08-10	56 / 75	Win32 EXE	flashplayer_install_cn.exe
2025-07-20	42 / 67	Android	951F41930489A8BFE963FCED5D8DFD79

Files Referring (2)

Scanned	Detections	Type	Name
2025-07-06	0 / 62	CSV	64a5243b9624d898caa86db0.csv
2024-12-29	0 / 61	XML	sharedStrings.xml

Historical Whois Lookups (4)

Last Updated	Organization	Email
--------------	--------------	-------

Answer : 951F41930489A8BFE963FCED5D8DFD79