Friday Overtime CTF

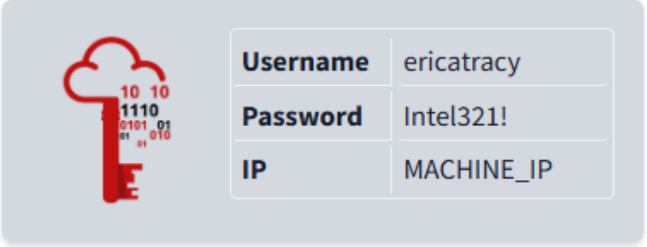
The artifacts in this scenario originate from an actual cyber-attack. For safety reasons, it is strongly recommended to interact with them only within the provided virtual machine (VM), which operates in a secure, isolated environment. This is a subscription only for TryHackMe users. It was created by 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:

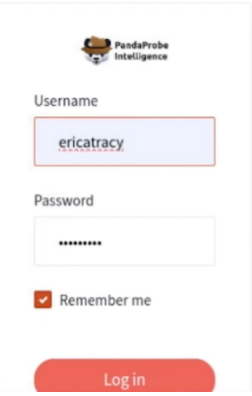
1. Downloading the malware samples provided in the ticket, ensuring they were contained in a secure environment.
2. Running the samples through preliminary automated malware analysis tools to get a quick overview.
3. Deep diving into a manual analysis, understanding the malware's behaviour, and identifying 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.



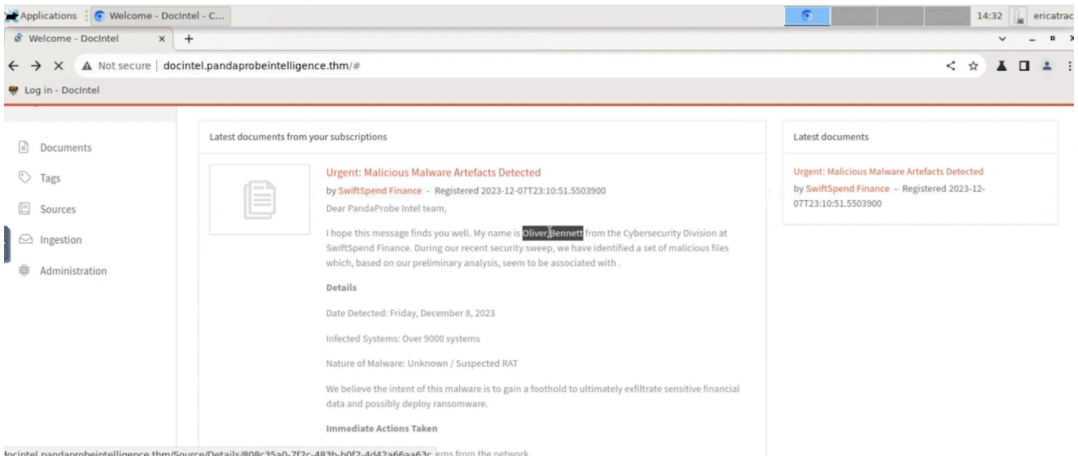
Muhammad Hisyam
Github - Cybersecurity Notes



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?

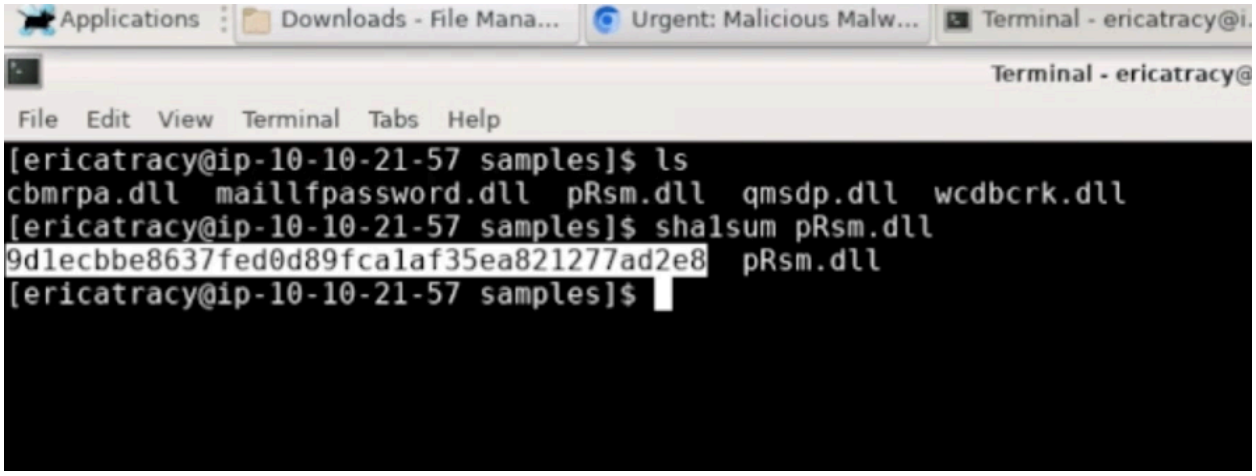


After logging into the DocIntel platform, you'll see the latest documents from your subscriptions displayed. Begin reviewing the emails/documents, and you should be able to quickly identify the sender's name.
Answer : Oliver Bennett

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.

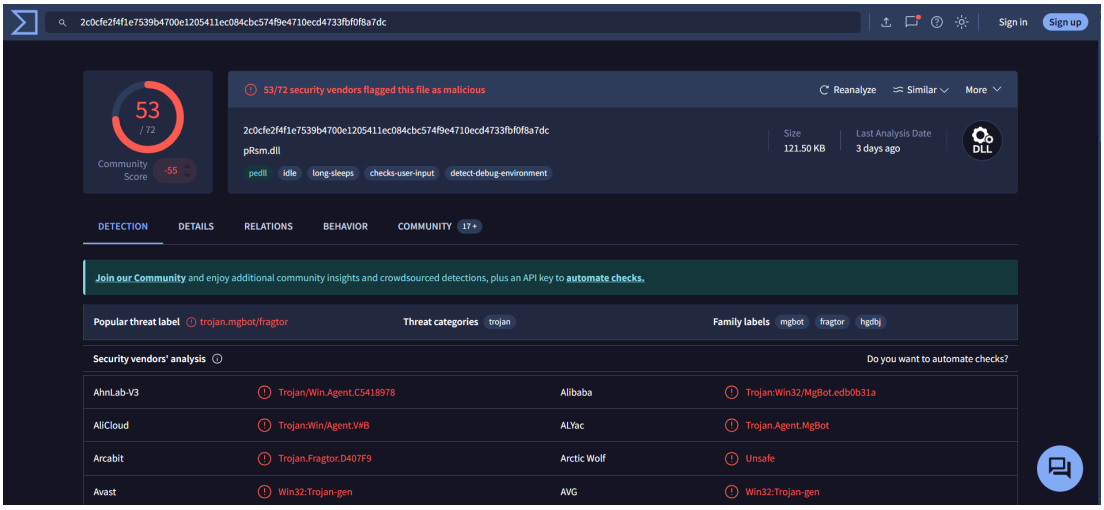
For the SHA1 hash of the file, we will use the command sha1sum pRsm.dll. Pressing enter will run the command and show the SHA1 hash.



Answer : 9d1ecbbe8637fed0d89fca1af35ea821277ad2e8

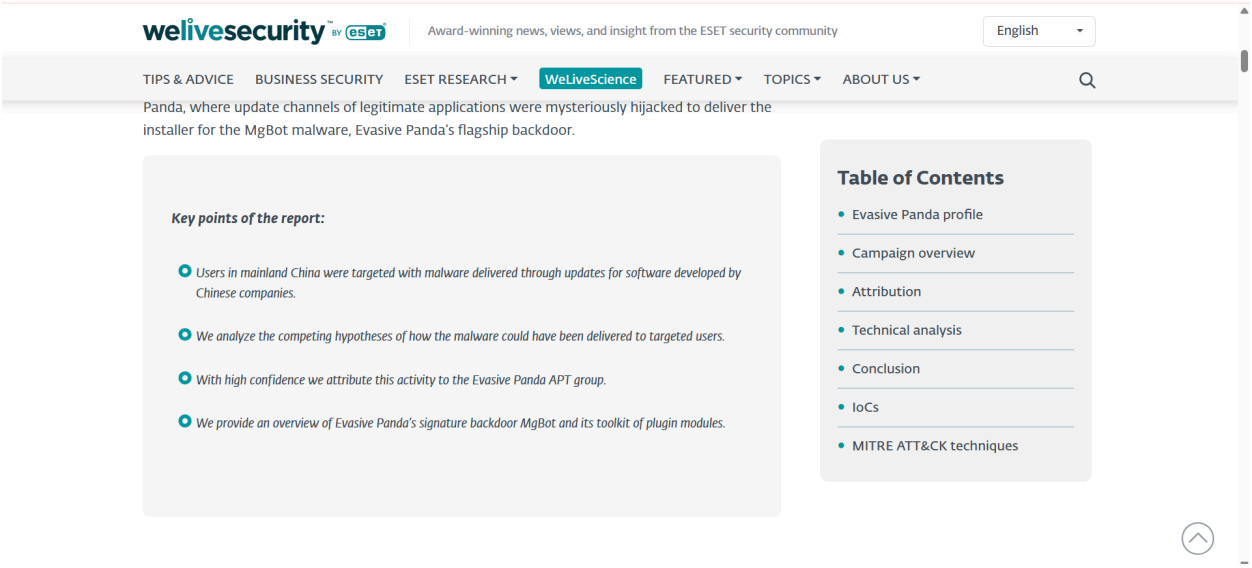
Which malware framework utilizes these DLLs as add-on modules?

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



Muhammad Hisyam
Github - Cybersecurity Notes

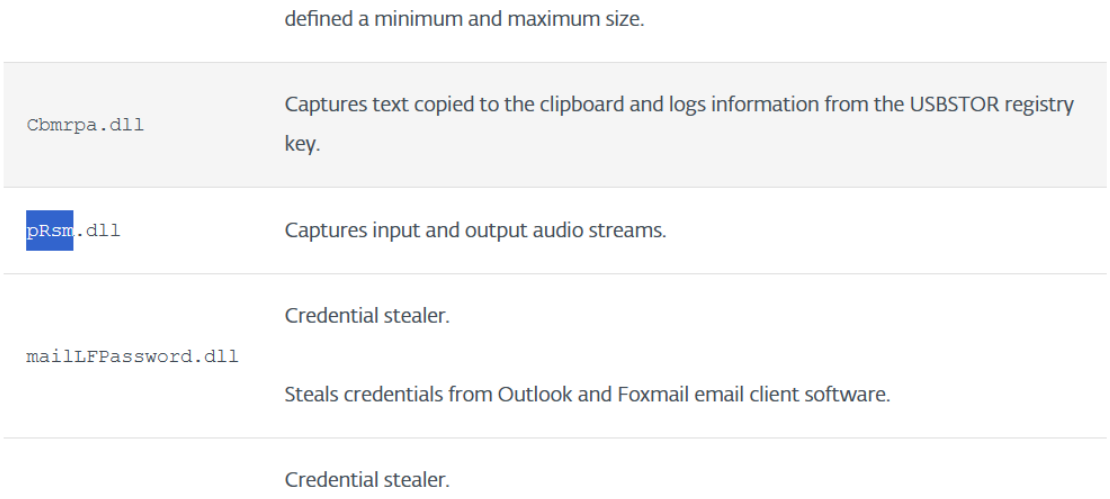
DLLs (Dynamic Link Libraries) are often used as modular components that extend the core functionality of the malware. Or we can find it by using search engines like google.



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.



T1560.002	Archive Collected Data: Archive via Library	MgBot's plugin module `sebasek.dll` uses aPLib to compress files staged for exfiltration.
T1123	Audio Capture	MgBot's plugin module `pRsm.dll` 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 download locations according to ESET telemetry

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

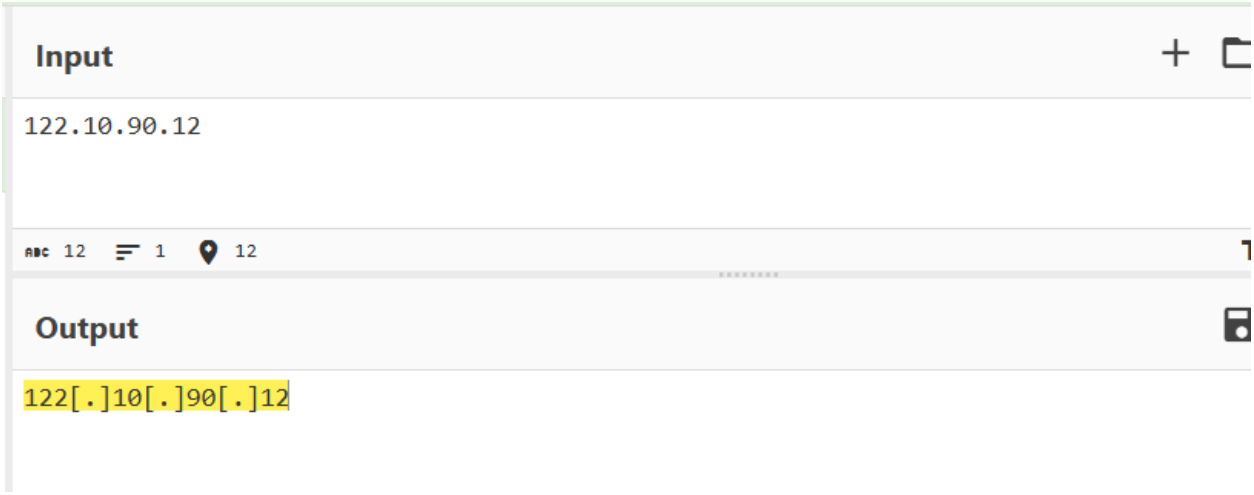
Answer : hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe

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.

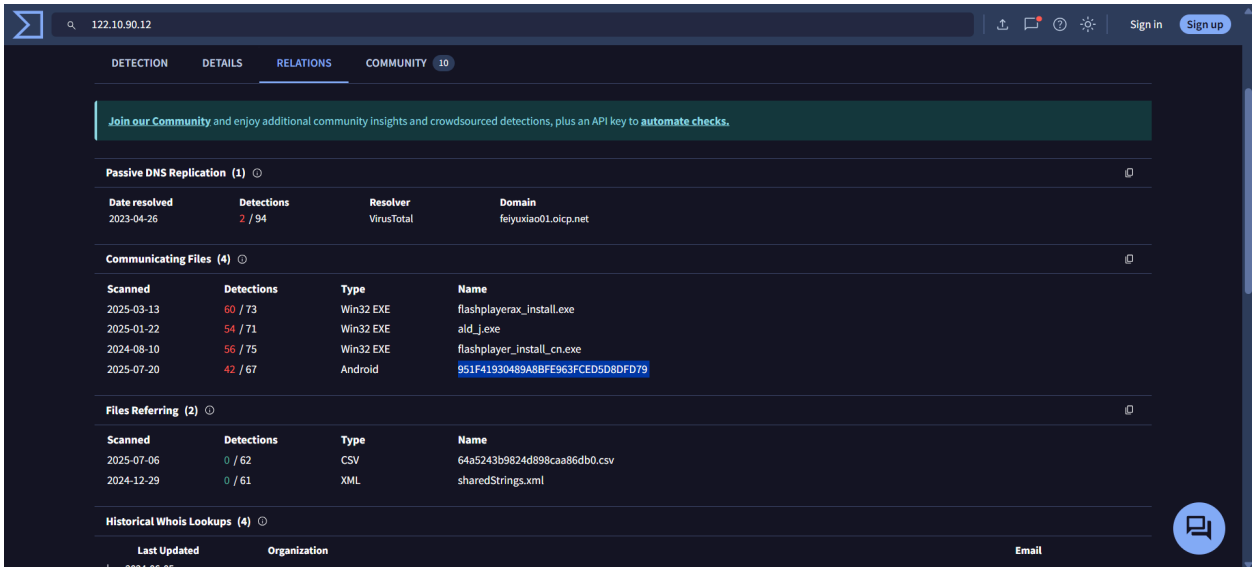


Make sure that we delete the square bracket when we input the IP address in cyberchef.

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.



Answer : 951F41930489A8BFE963FCED5D8DFD79