Friday Overtime - THM writeups (premium room)

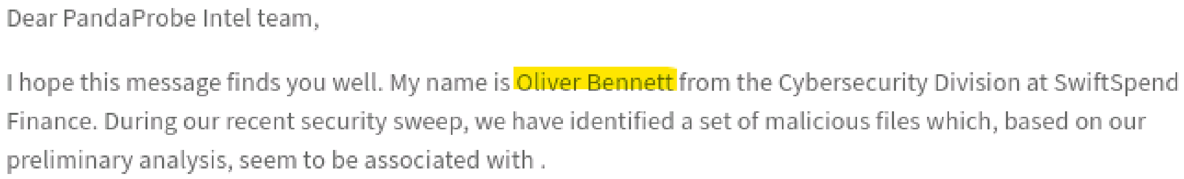
Created	@August 5, 2025 8:39 PM
Tags	

Disclaimer: The artefacts used in this scenario were retrieved from a real-world cyber-attack. Hence, it is advised that interaction with the artefacts be done only inside the attached VM, as it is an isolated environment.

A room that introduces me into CTI.

1. **Who shared the malware samples?**

   The document shared has the name of the sender at the beginning of the message.

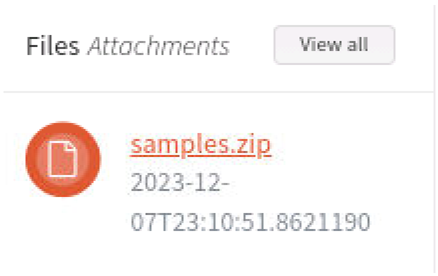


Dear PandaProbe Intel team,

I hope this message finds you well. My name is Oliver Bennett from the Cybersecurity Division at SwiftSpend Finance. During our recent security sweep, we have identified a set of malicious files which, based on our preliminary analysis, seem to be associated with .

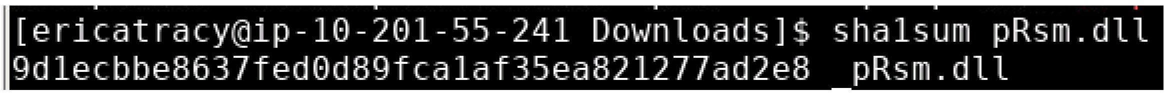
Answer: Oliver Bennet

2. **What is the SHA1 hash of the file "pRsm.dll" inside samples.zip?**



samples.zip
2023-12-07T23:10:51.8621190

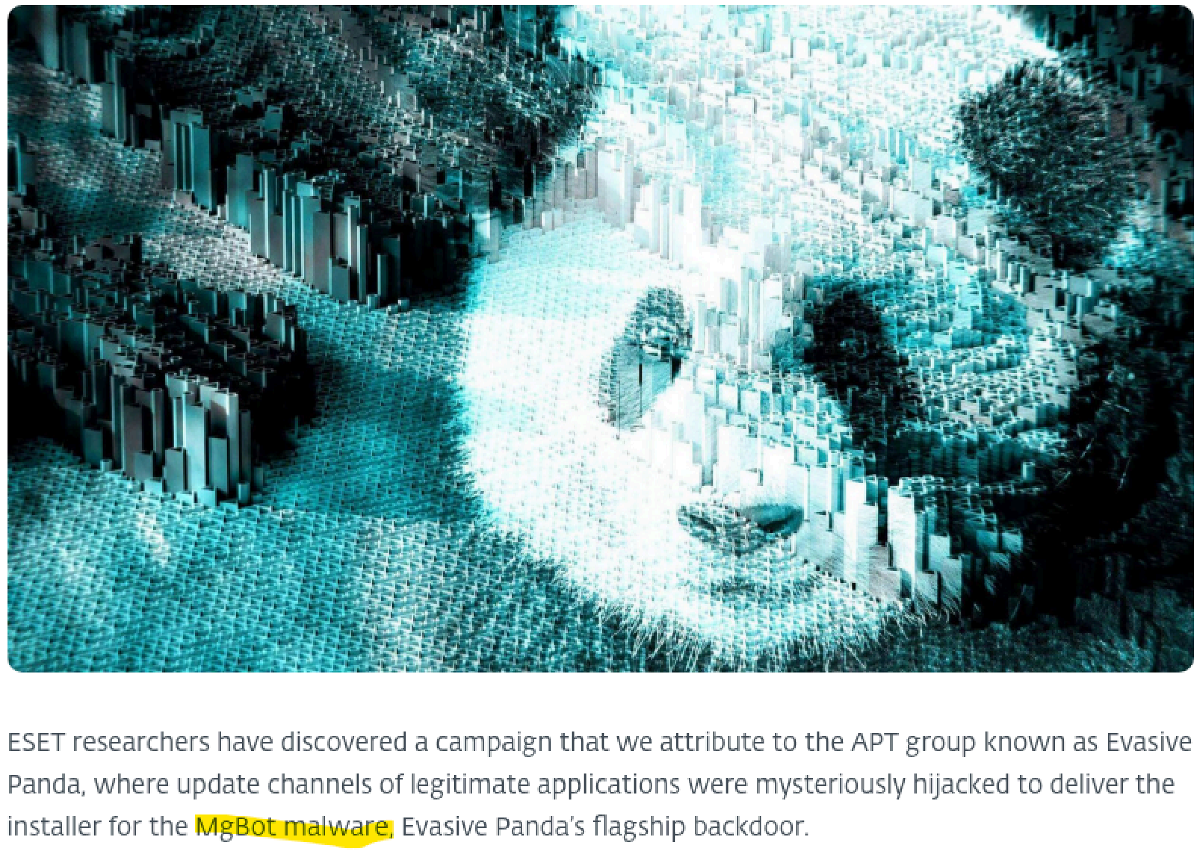
After downloading the file and unzipping it using the password provided in the message, we then can use sha1sum to get the SHA1 hash of the pRsm.dll file.



```
[ericatracy@ip-10-201-55-241 Downloads]$ sha1sum pRsm.dll
9d1ecbbe8637fed0d89fca1af35ea821277ad2e8  pRsm.dll
```

Answer: 9d1ecbbe8637fed0d89fca1af35ea821277ad2e8

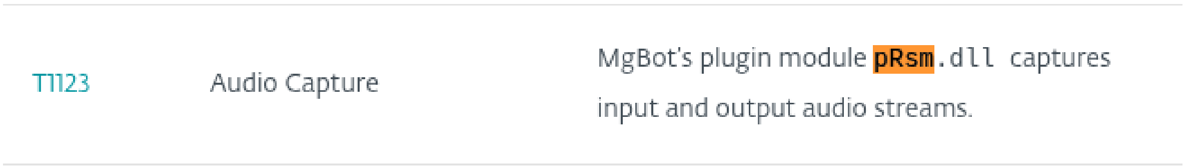
3. **Which malware framework utilizes these DLLs as add-on modules?**
   I searched up on google “prsm dll” and got an article on **welivesecurity** as the top search return, and after reading the article for a bit I found the answer.



ESET researchers have discovered a campaign that we attribute to the APT group known as Evasive Panda, where update channels of legitimate applications were mysteriously hijacked to deliver the installer for the MgBot malware, Evasive Panda's flagship backdoor.

Answer: MgBot

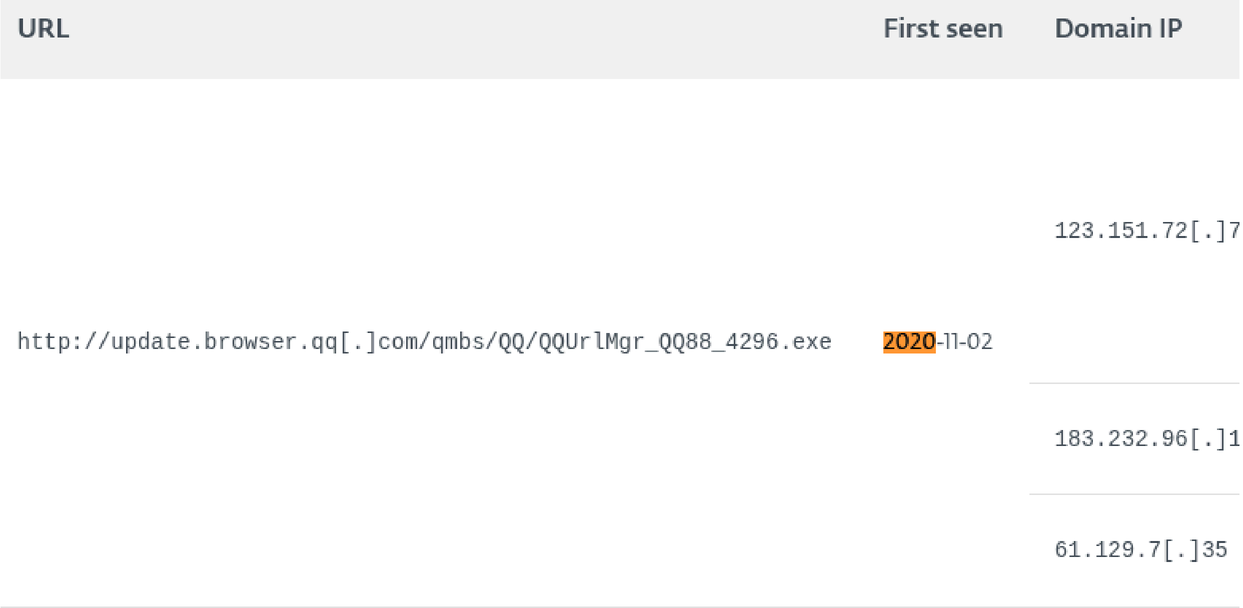
4. **Which MITRE ATT&CK Technique is linked to using pRsm.dll in this malware framework?**
   Using Ctrl + F to search for "pRsm.dll", the answer lays under **MITRE ATT&CK** section in the article.



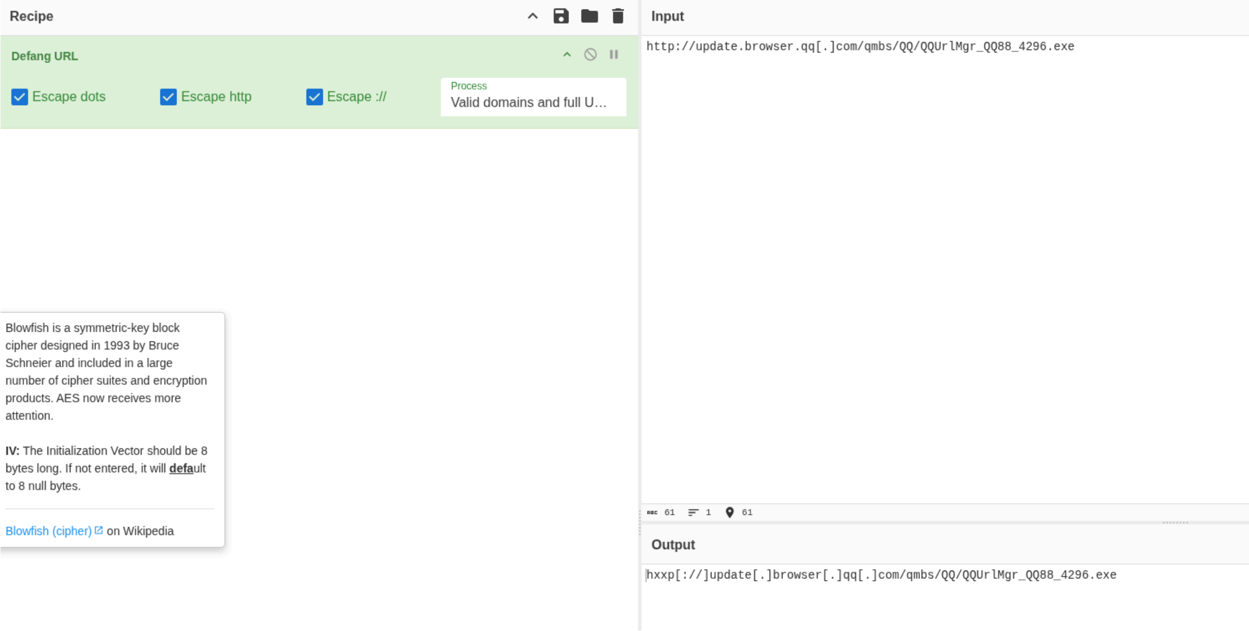
T1123	Audio Capture	MgBot's plugin module `pRsm.dll` captures input and output audio streams.

Answer: T1123

5. **What is the CyberChef defanged URL of the malicious download location first seen on 2020-11-02?**
   We can find the answer in the **Technical analysis** section of the article. We can then use Cyberchef to defang the URL.



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



Recipe

Defang URL

☑ Escape dots ☑ Escape http ☑ Escape ://

Process: Valid domains and full U…

Input

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

Output

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

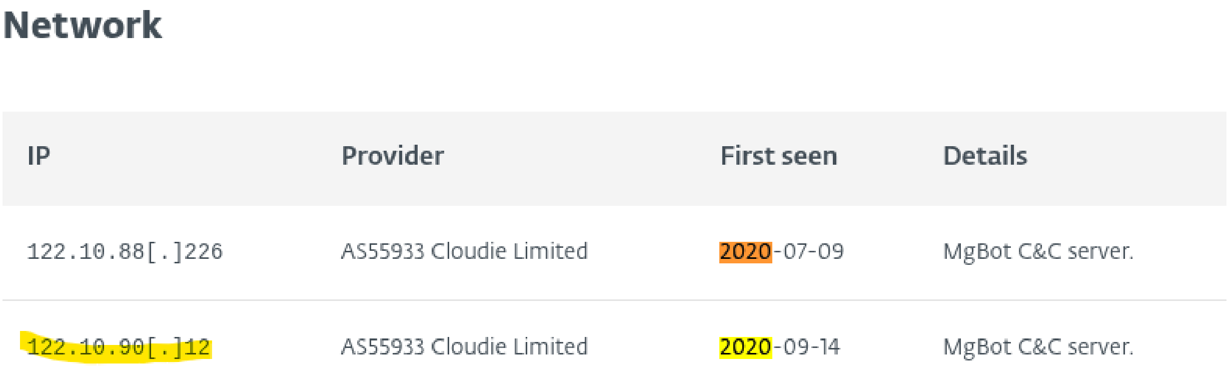
Blowfish is a symmetric-key block cipher designed in 1993 by Bruce Schneier and included in a large number of cipher suites and encryption products. AES now receives more attention.

IV: The Initialization Vector should be 8 bytes long. If not entered, it will **defa**ult to 8 null bytes.

Blowfish (cipher) on Wikipedia

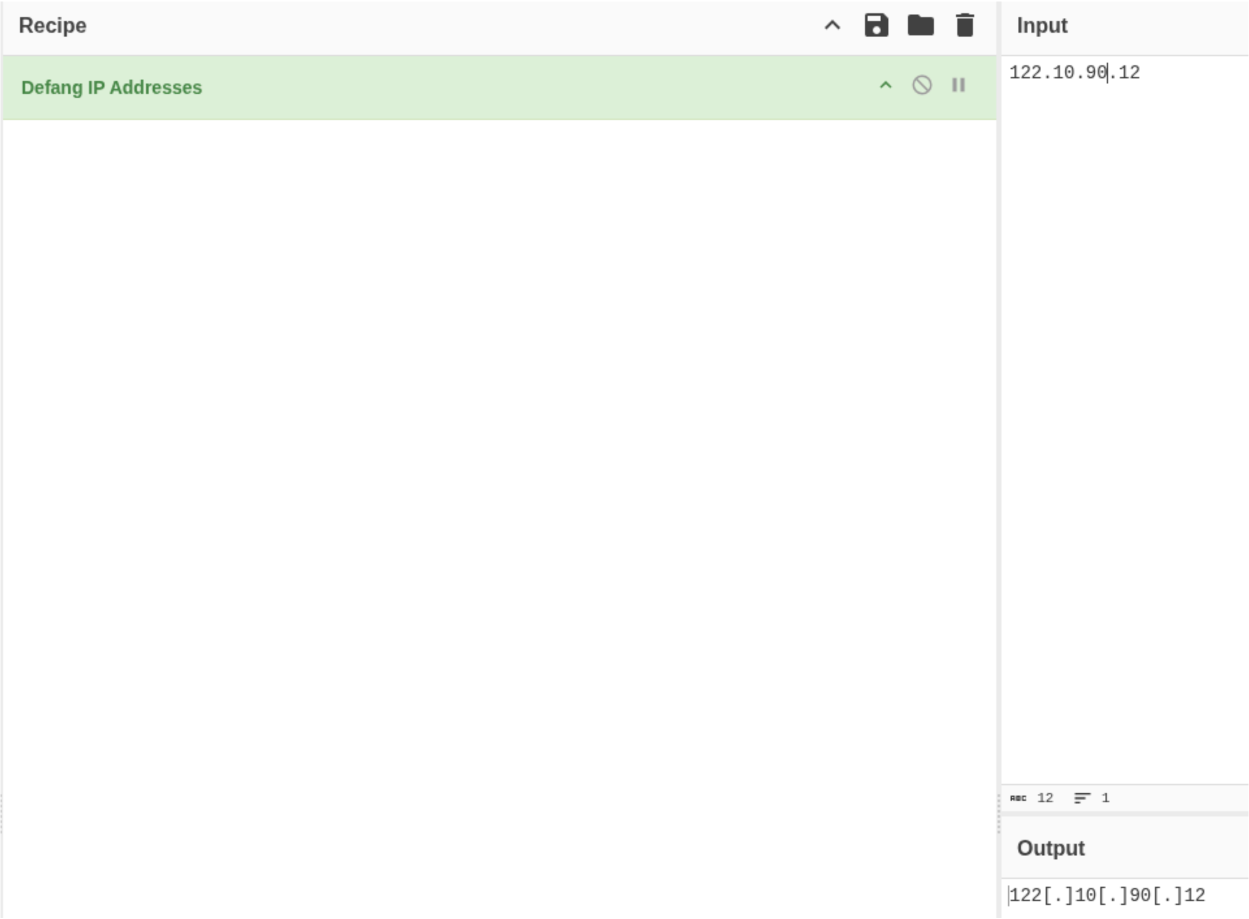
Answer:
hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296[.]exe

6. **What is the CyberChef defanged IP address of the C&C server first detected on 2020-09-14 using these modules?**
   Similar to the previous question, we can find the IP under the **Network** section of the article, then we can copy it over to Cyberchef to defang the IP.



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.

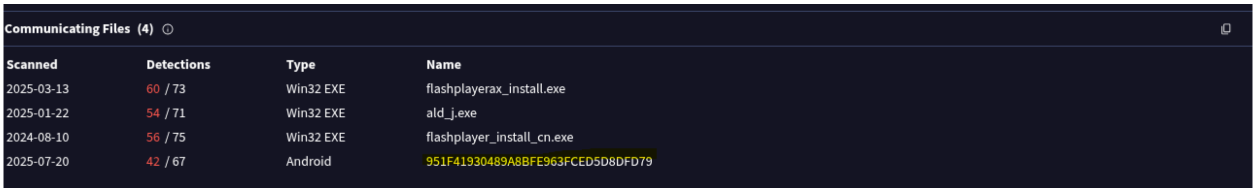


```
122.10.90.12
```

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

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

7. **What is the md5 hash of the spyagent family spyware hosted on the same IP targeting Android devices in Jun 2025?**
   Since the IP above was the MgBot C&C server IP, we might be able to find something on **virustotal**. Paste the defanged IP into virustotal, and go to the relations tab, we can find an “Android” communicating file with it’s md5 hash.



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

Answer: 951F41930489A8BFE963FCED5D8DFD79