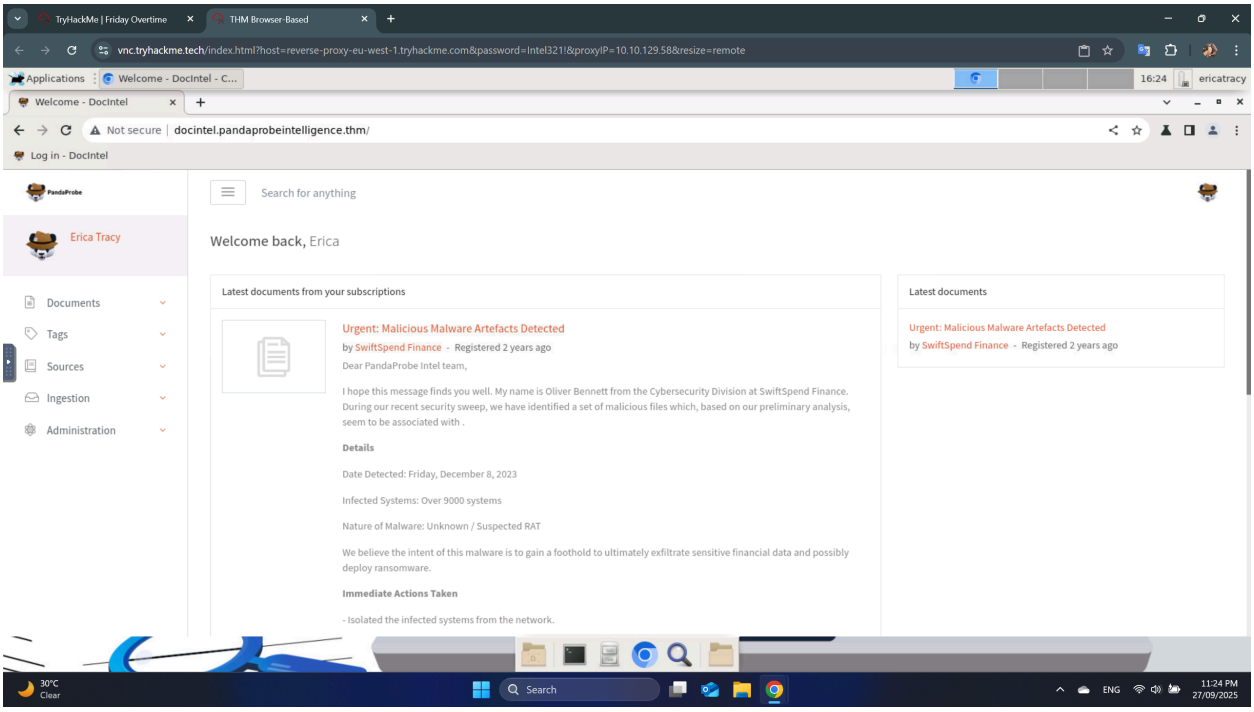
Friday Overtime

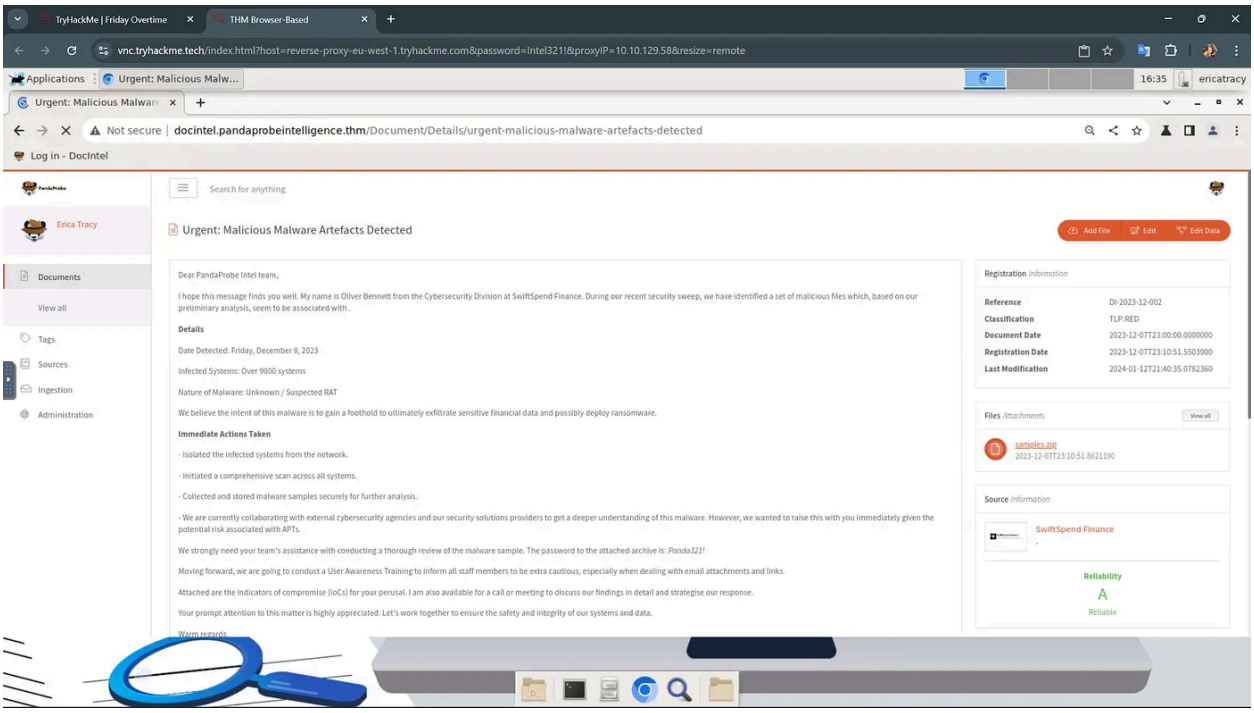
Step into the shoes of a Cyber Threat Intelligence Analyst and put your investigation skills to the test.

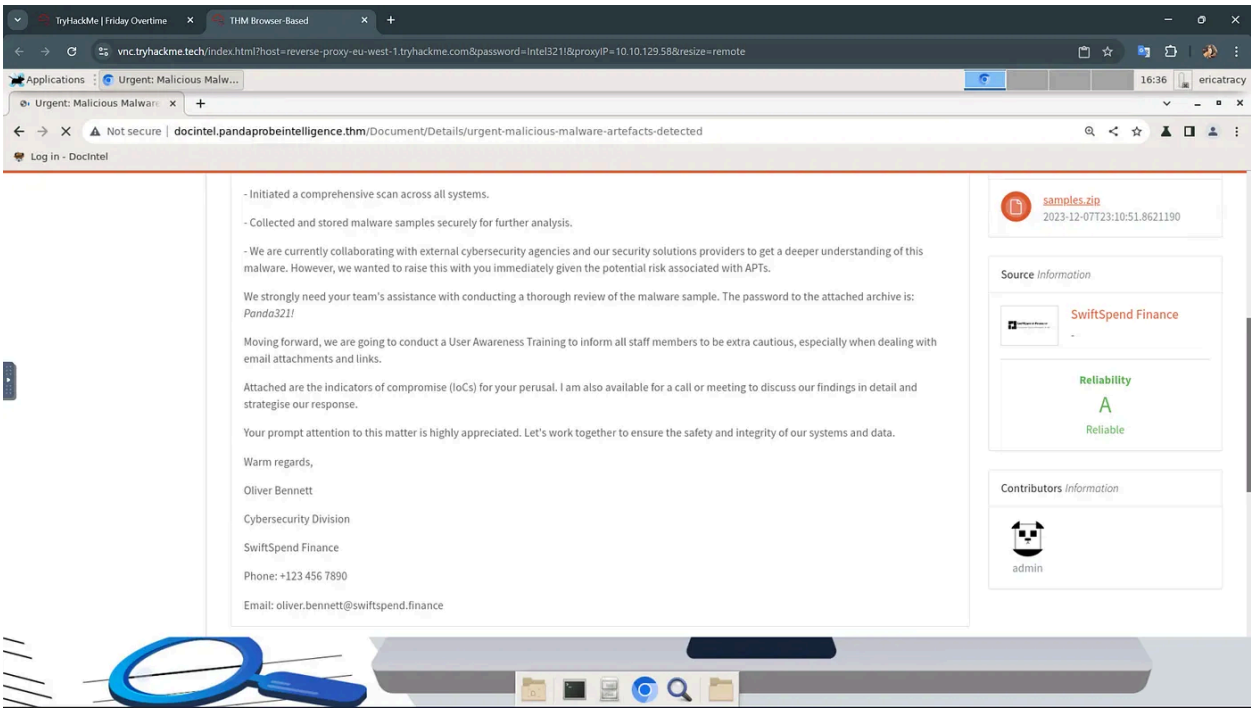
In this challenge, we will be assuming the rule of a CTI (Cyber Threat Intelligence) analyst, investigating a ticket by a member of the security division at the company.

We start the challenge by inspecting the ticket we were left by the security department, which has the details of the attempted attack along with the malicious artefacts in a .zip file.



When we open the document, we see the full email, along with *samples.zip* that we can download to analyze.





Just by reading the email, we are presented with the answer of the first question.

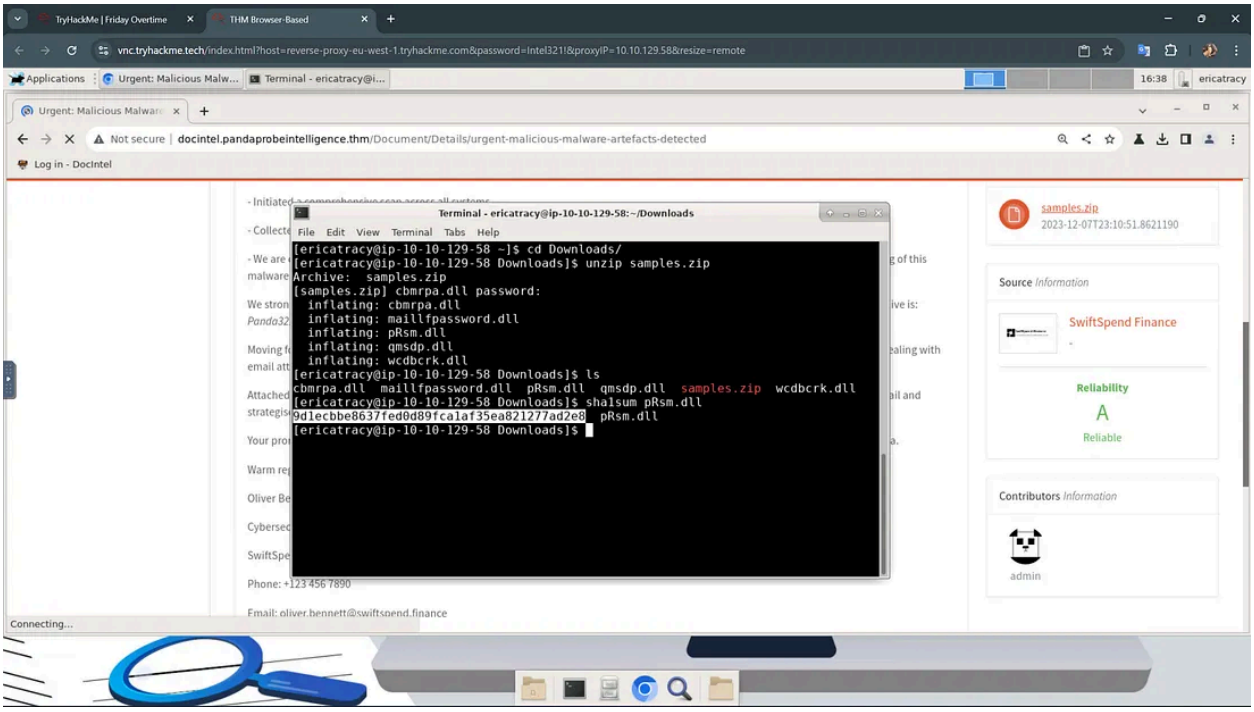
> Who shared the malware samples?

Answer: **Oliver Bennett**

We then download the sample.zip folder, unzip it and inspect what we find. We got several .dll files. Simply put, a DLL (Dynamic-Link Library) file is a library that contains code and data that can be used by several programs and processes on the MS Windows OS. They are one of the most common file types to be used as malicious files.

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

We can get the answer by unzipping the folder then calculating the SHA1 hash of this file.

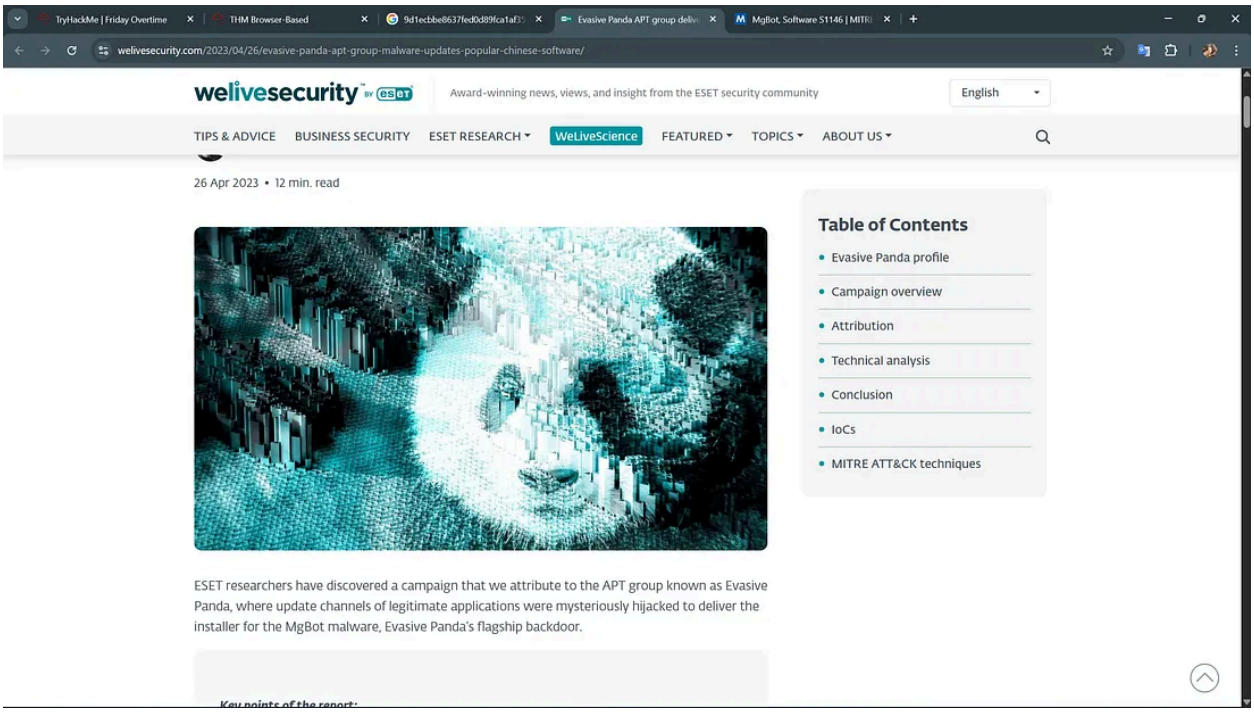


Answer: **9d1ecbbe8637fed0d89fca1af35ea821277ad2e8**

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

If we searched for pRsm.dll, we’ll have this article be ESET as the first search result.

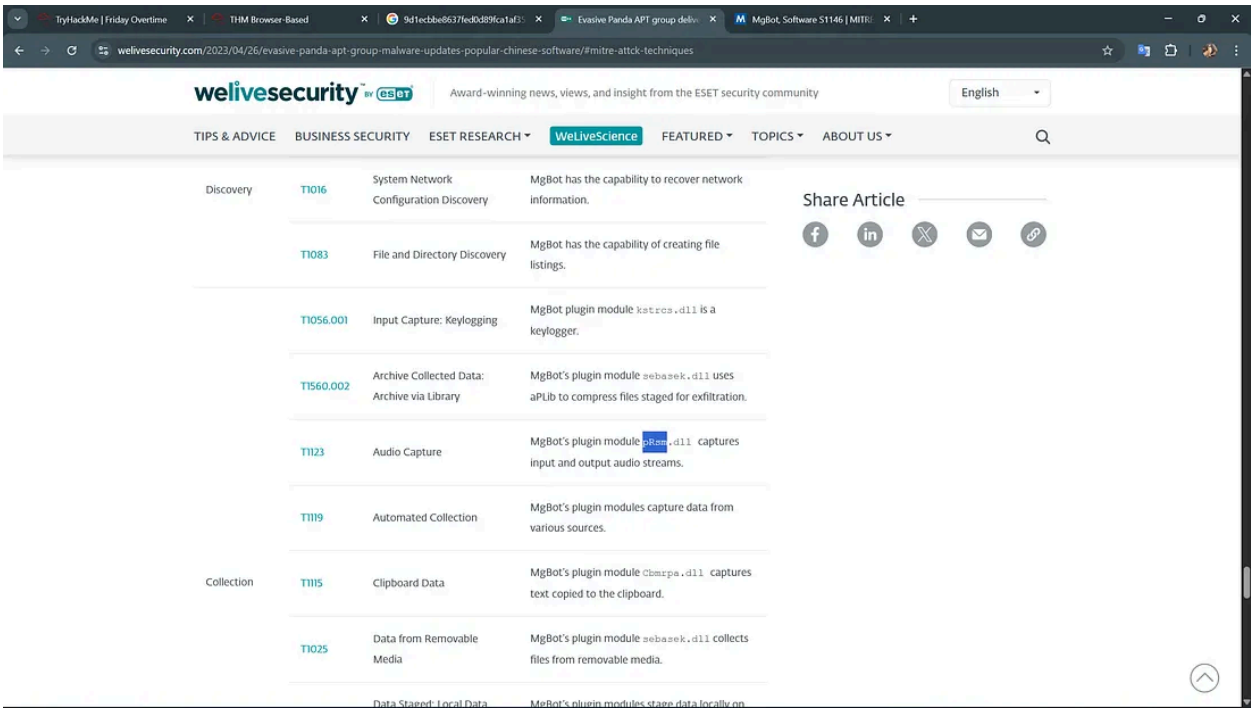
Going through it, we find the malware framework that used these DLLs.



Answer: **MgBot**

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

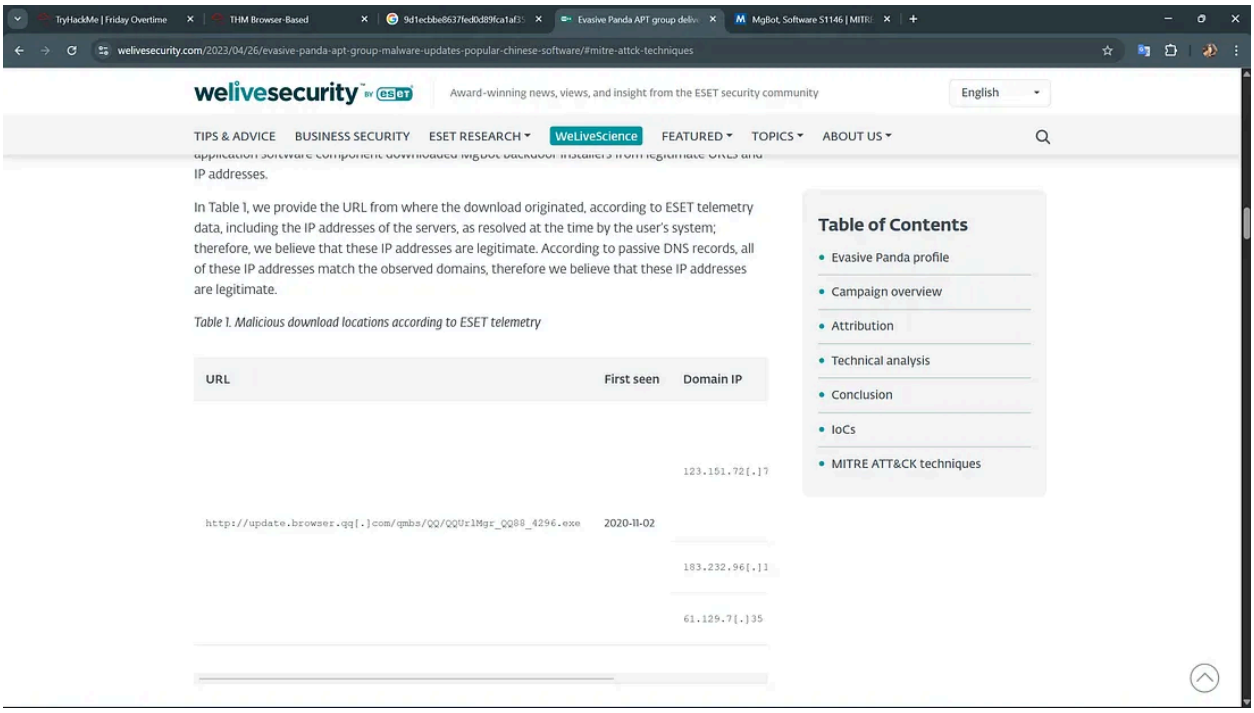
Searching for pRsm.dll in the article using **Ctrl + F**, we find the MITRE ATT&CK Technique used by this file.



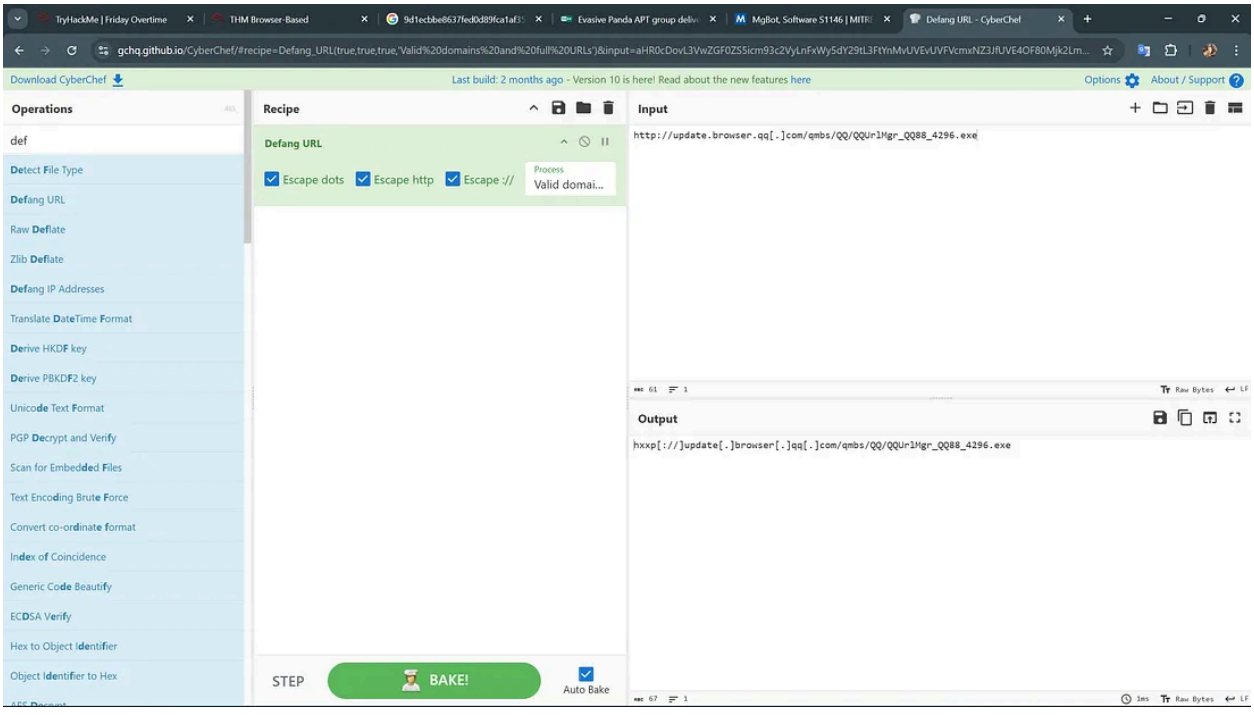
Answer: **T1123**

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

If we go through the article, we will come across a *"Technical Analysis"* section that provides the URL from where the download originated, according to ESET telemetry data.



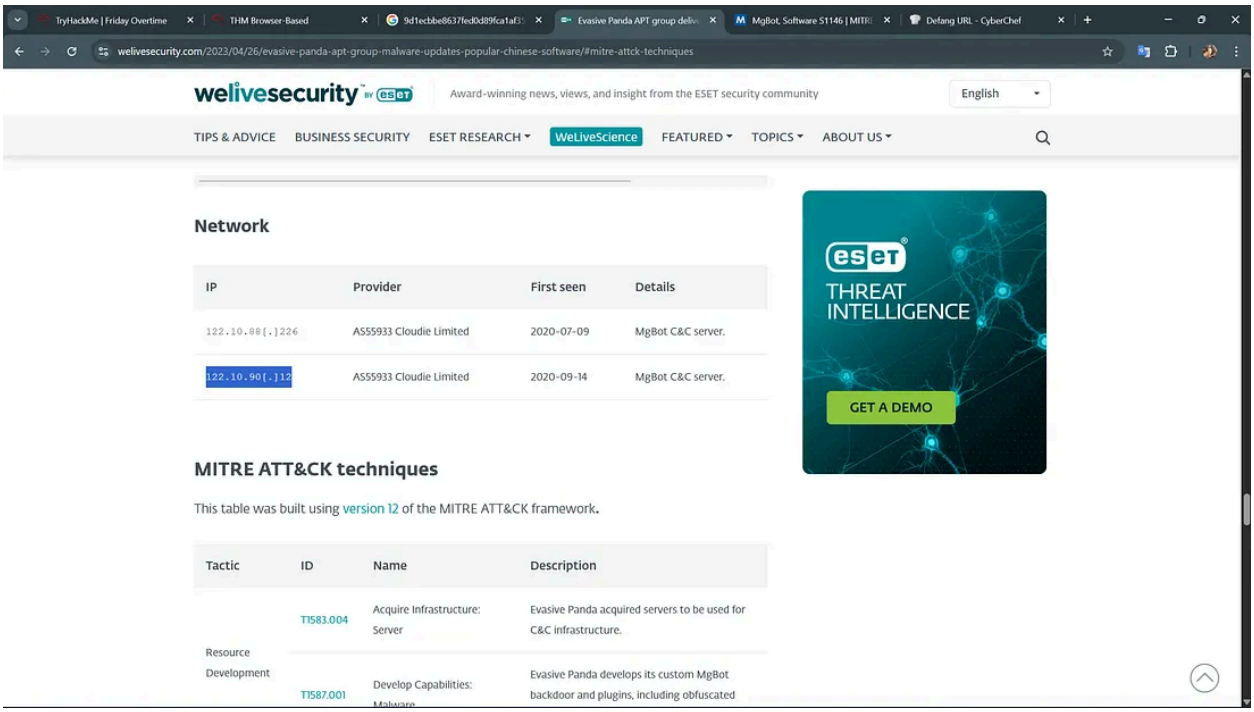
We then copy the URL and go to CyberChef to defang it. To defang a URL is to modify a potentially harmful link, making it non-functional and safe to share.



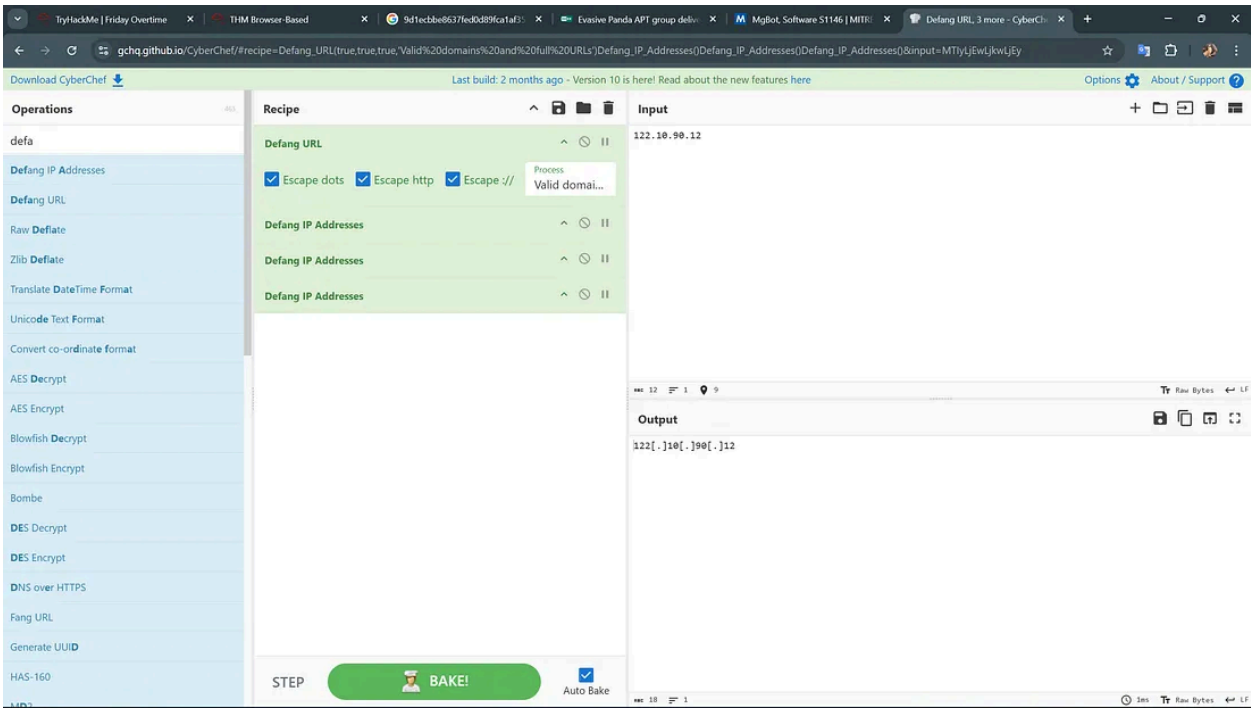
Answer: **hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296[.]exe**

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

In the "*IoCs*" section of the article, we find a table of network IoCs, containing the IP address of the C2 server first detected on the specified date.



We repeat the 'defanging' process using CyberChef, this time for the IP address.

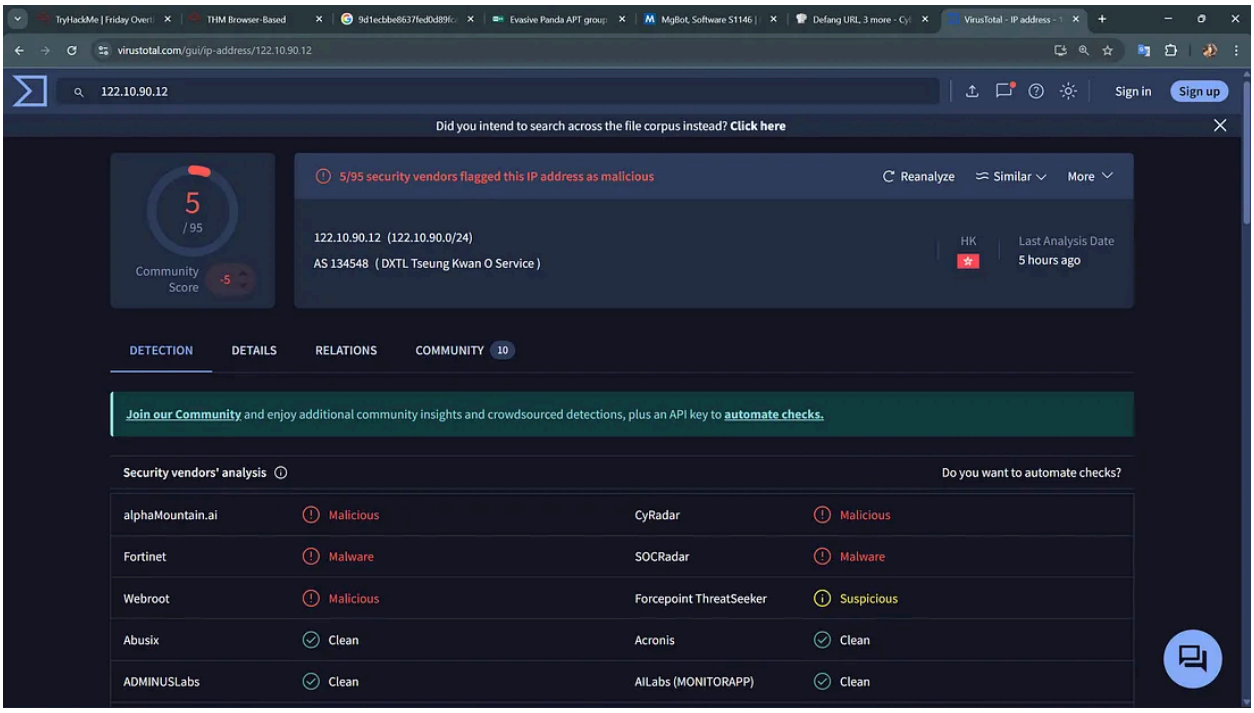


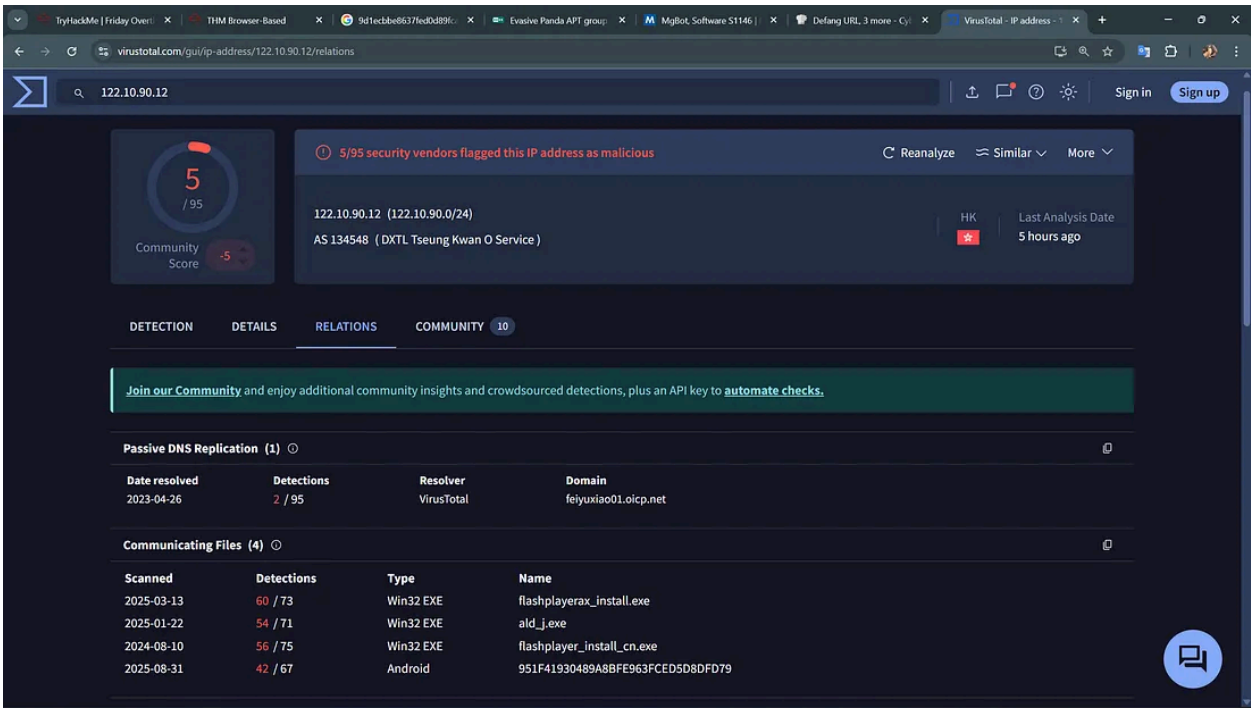
Answer: **122[.]10[.]90[.]12**

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

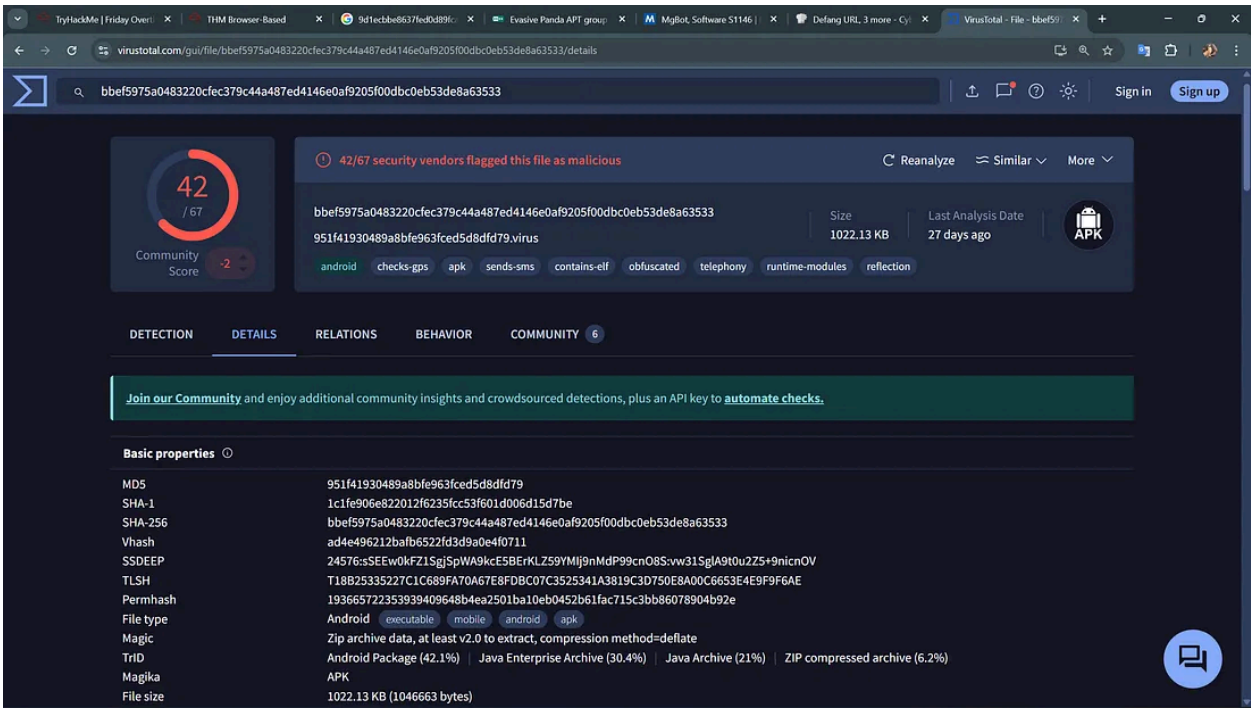
For this question, we can use any reputation checker to see data related to this IP address. We'll use the one and only *VirusTotal*. We search for the IP address on VT, and go to the "*Relations*" tab where we can find related info.

Press enter or click to view image in full size



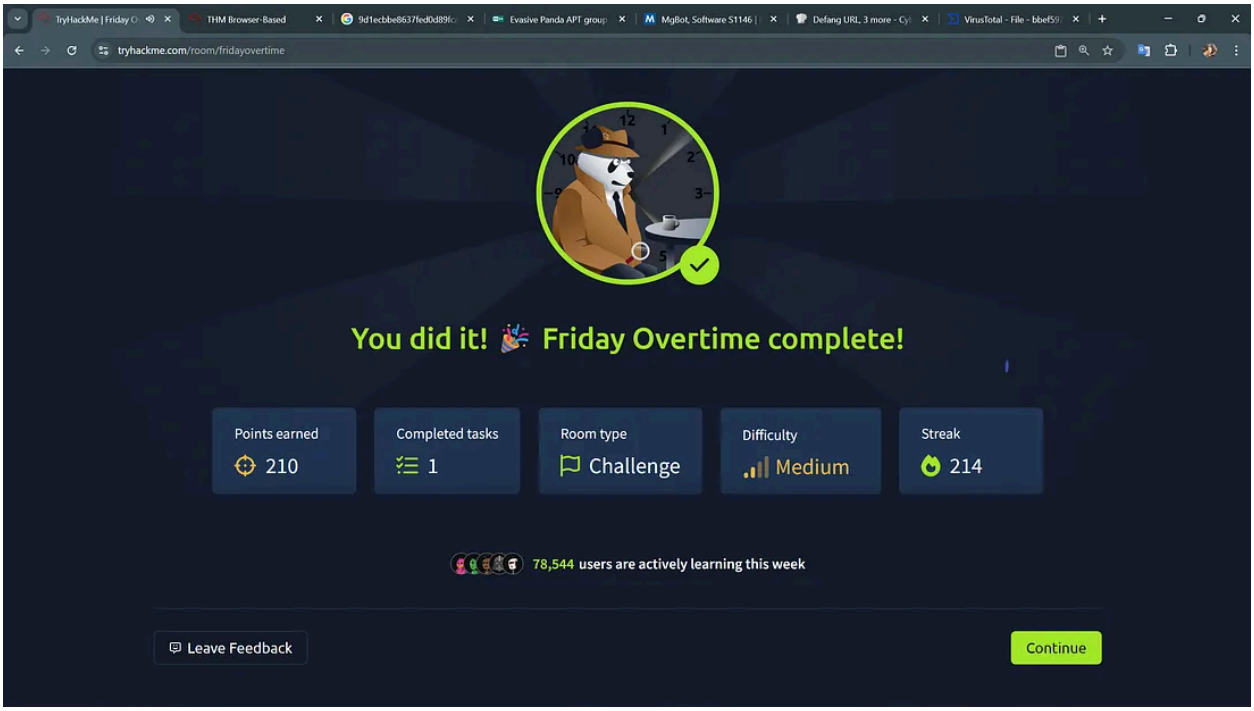


We find a file related to this IP address whose Type is Android. When we click on it name, we are directed to a separate page for this malware. On the "*Details*" tab, we find its MD5 hash and therefore our final answer.



Answer: **951F41930489A8BFE963FCED5D8DFD79**

Et Voilà!



This was a straightforward challenge with no need to use any special tools, only your Threat Intel mindset, and the mighty Virus Total!