Introduction

Welcome to my walkthrough of the **Friday Overtime** on Tryhackme . This guide will take you step-by-step through the challenge, providing detailed explanations and solutions for each task. By the end of this walkthrough, you should have a solid understanding of how to approach and solve this type of challenge.

Q: Who shared the malware samples?

on the docintel dashboard we can see the the name of person who shared us malware samples .

Warm regards,

Oliver Bennett

Cybersecurity Division

SwiftSpend Finance

Phone: +123 456 7890

A: Oliver Bennett

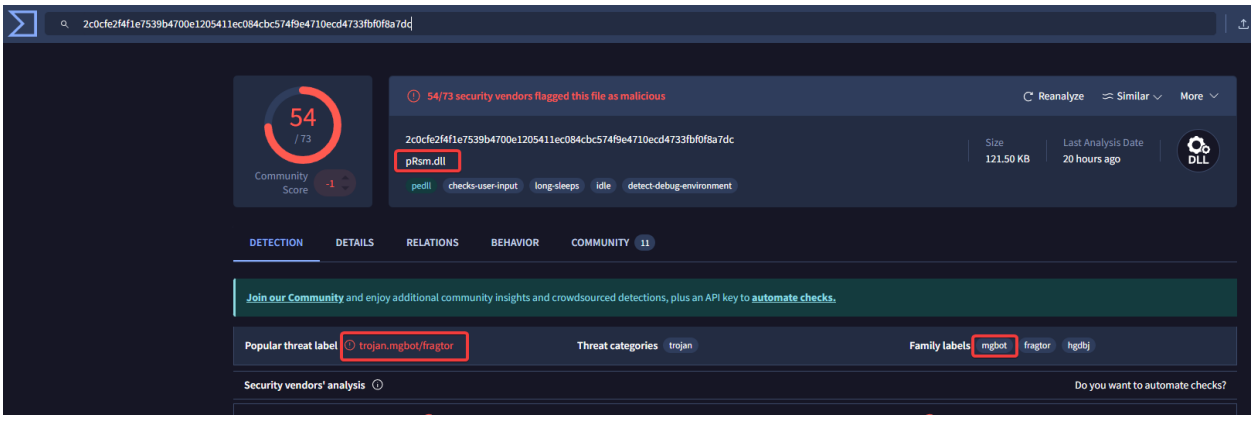
Q: What is the SHA1 hash of the file “pRsm.dll” inside samples.zip?

download the sample.zip file attached with that mail , unzip it with the password that given in mail already “Panda321!” and type command with terminal sha1sum “filename” .

A: 9d1ecbbe8637fed0d89fca1af35ea821277ad2e8

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

check this hash in virustotal and we can see the malware framework of these dlls .



A: Mgbot

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

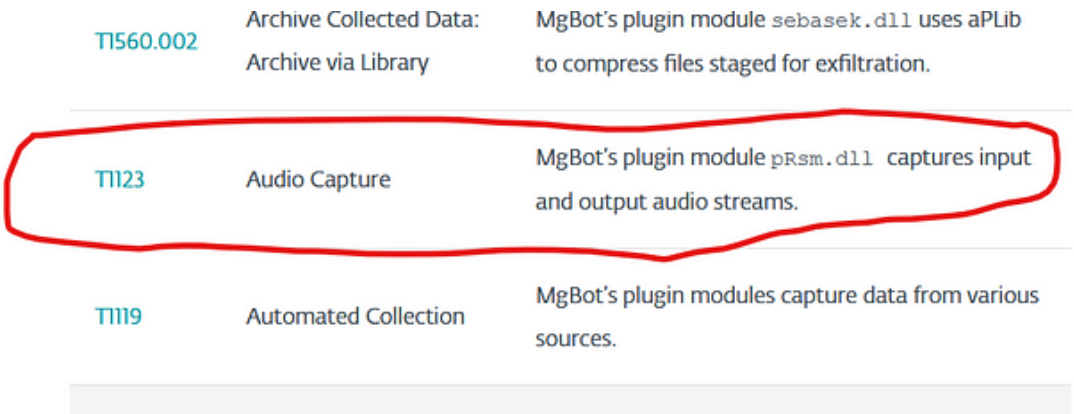
now we have to do some OSINT like things . just search for Mgbot on web-browser and found some article.

Evasive Panda APT group delivers malware via updates for popular Chinese software

ESET Research uncovers a campaign by the APT group known as Evasive Panda targeting an international NGO in China with...

www.welivesecurity.com

reading this article and found that which technique that dll file linked with .



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.

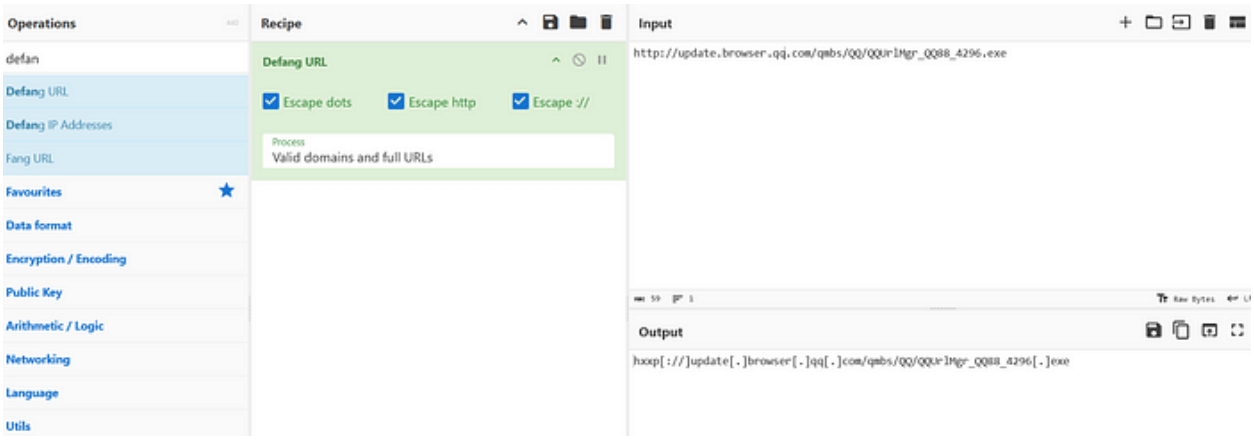
A: T1123

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

on that article that url is given us already with Date just copy it and open the cyberchef and search for "defang URL" . and defang the URL

Table 1. Malicious download locations according to ESET telemetry

URL	First seen	Domain IP	ASN	Downloader
http://update.browser.qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296.exe	2020-11-02	123.151.72[.]74	AS58542	QQUrlMgr.exe QQ.exe QQLive.exe QQCall<XX>.exe
		183.232.96[.]107	AS56040	
		61.129.7[.]35	AS4811	



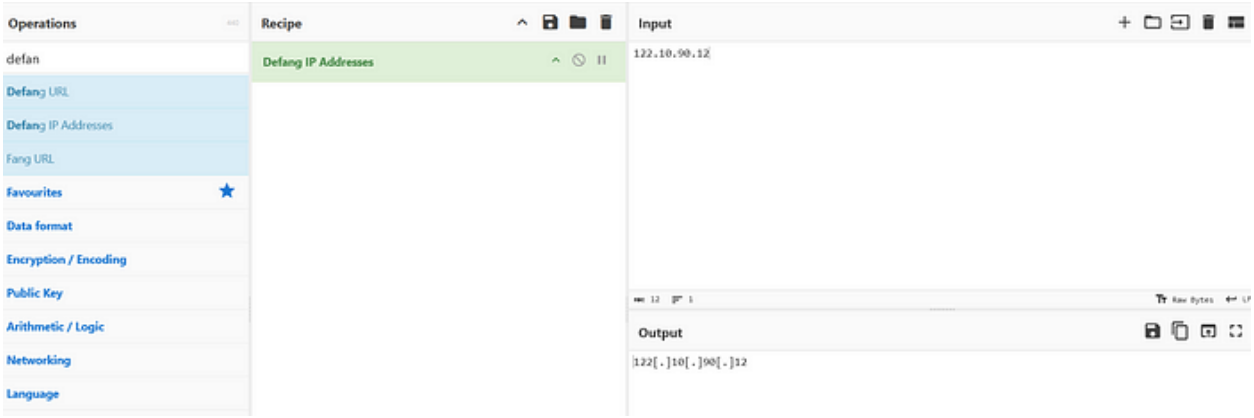
A: hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr_QQ88_4296[.]exe

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

By searching for the date "2020–09–14" in the network session, we can locate the C2 server IP address, which can then be defanged using CyberChef (defang IP addresses).

Network

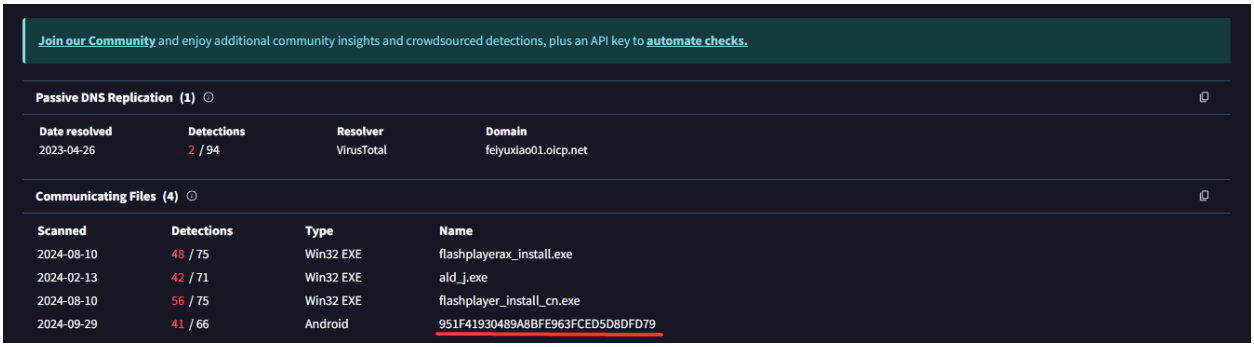
IP	Provider	First seen	Details
122.10.88[.]226	AS55933 Cloudie Limited	2020-07-09	MgBot C&C server.
122.10.90[.]12	AS55933 Cloudie Limited	2020-09-14	MgBot C&C server.



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

Q: What is the SHA1 hash of the spyagent family spyware hosted on the same IP targeting Android devices on November 16, 2022?

search the previous IP of C2 server on virustotal where we can find the relations of this IP in relations session and click on Android name link and get the SHA1 hash of spyware in Details session .



Under the details tab of the android link, you will see the hashes

A: 1c1fe906e822012f6235fcc53f601d006d15d7be