Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

fridayovertime – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | fridayovertime – Enrico Santarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 02/10/2024 |
| **Link** | https://tryhackme.com/r/room/fridayovertime |

|  |  |  |
| --- | --- | --- |
| **Redação** | Enrico Santarelli | Membro |
| **Revisão** | João Branco | Presidente |
| **Aprovação** | João Branco | Presidente |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 01/10/2024 | Produção |
| **1** | 02/10/2024 | Revisão |
| **2** | 02/10/2024 | Aprovação |

**Sumário**

Contextualização 3

Desenvolvimento 3

Who shared the malware samples? 3

What is the SHA1 hash of the file "pRsm.dll" inside samples.zip? 4

Which malware framework utilizes these DLLs as add-on modules? 5

Which MITRE ATT&CK Technique is linked to using pRsm.dll in this malware framework? 5

What is the CyberChef defanged URL of the malicious download

location first seen on 2020-11-02? 5

What is the CyberChef defanged IP address of the C&C server

first detected on 2020-09-14 using these modules? 6

What is the SHA1 hash of the spyagent family spyware hosted

on the same IP targeting Android devices on November 16, 2022? 6

Conclusão 7

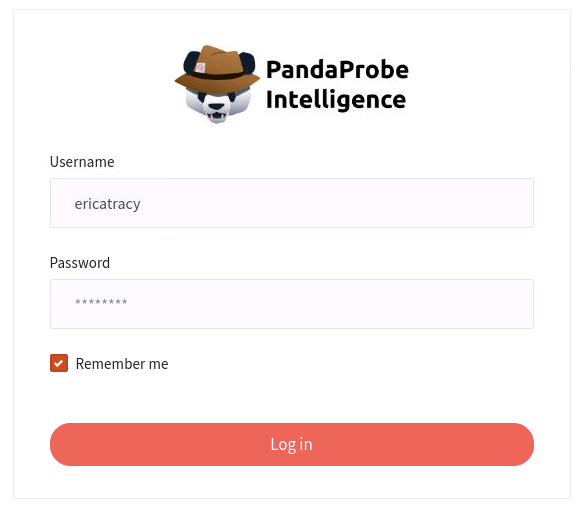
Referências 7

**Contextualização**

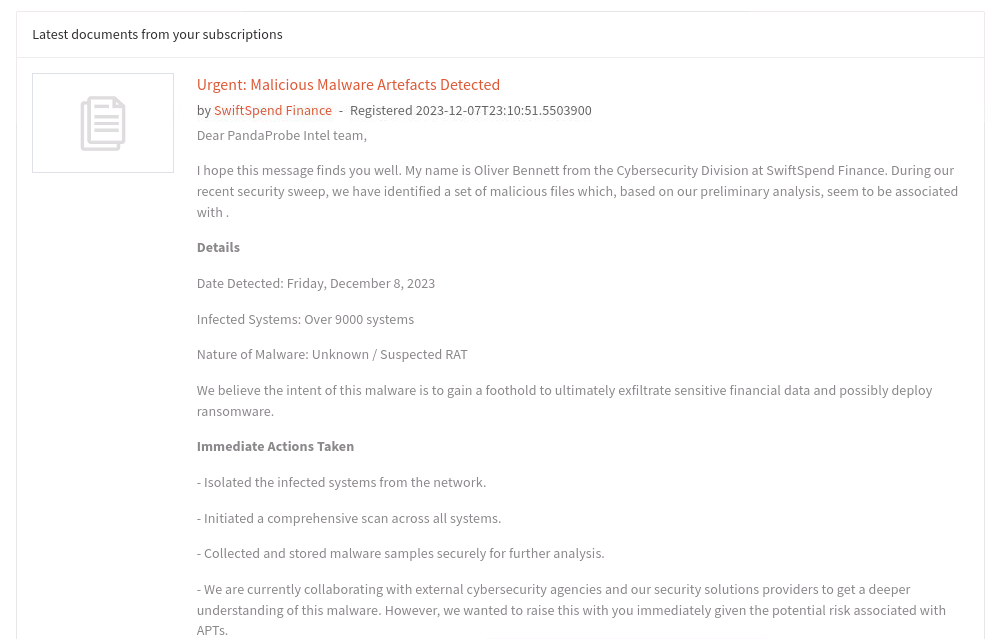
O CTF compões a trilha de SOC Level 1. A ideia dele é simular um problema de Threat Intelligence real, criando um ambiente de análise de um arquivo de malware. O CTF é de nível fácil e é ideal para aqueles que estão iniciando os estudos em Blue Team, principalmente em CTI.

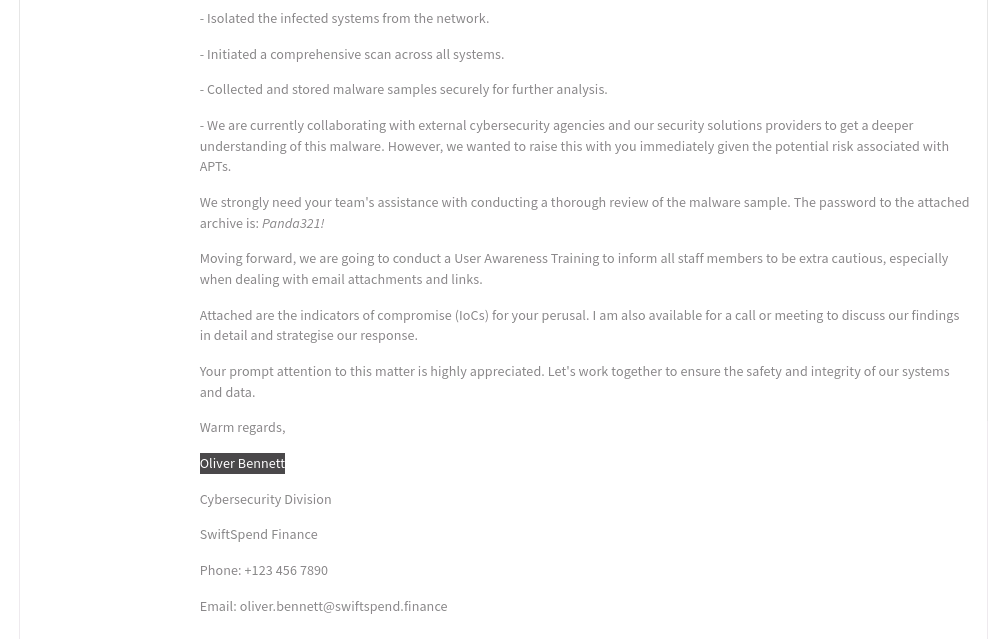
**Desenvolvimento**

**Who shared the malware samples?**



Na tela inicial, nos deparamos com uma mensagem de alerta a respeito da detecção de um malware em vários sistemas da rede.



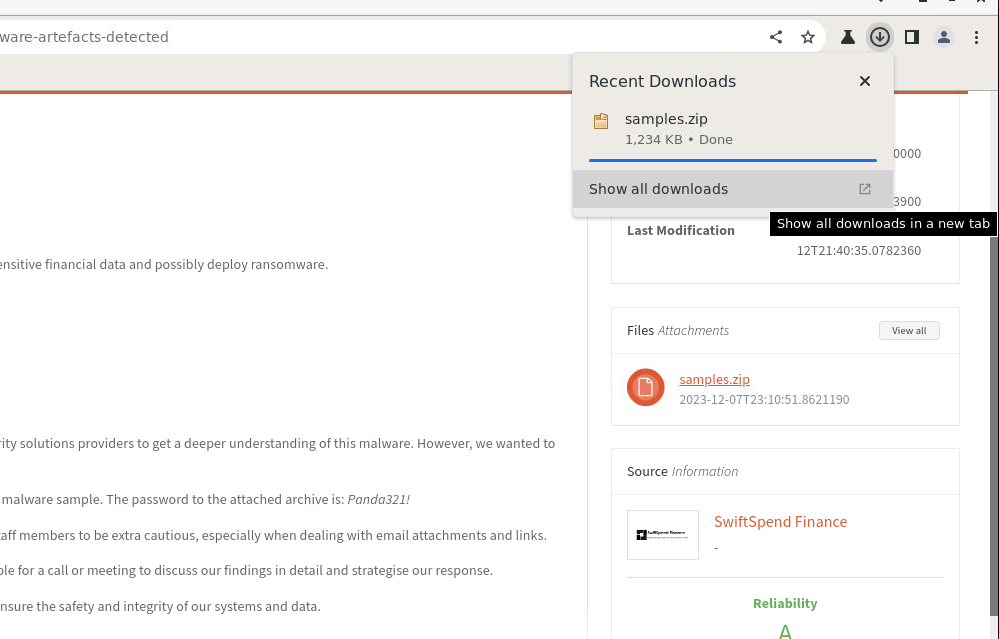


Dessa mensagem é possível extrair que o autor do e-mail que compartilhou as amostras do malware é o Oliver Bennett.

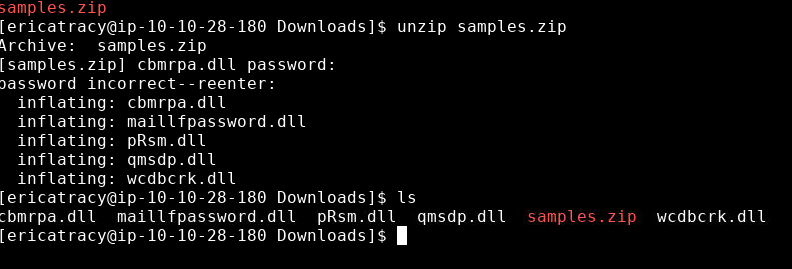
R: Oliver Bennett.

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

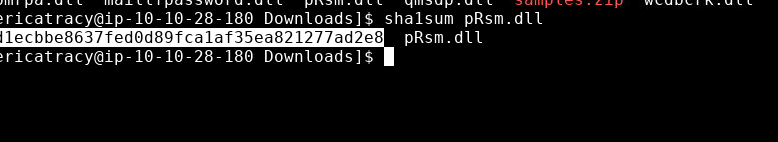
Primeiro, baixamos o arquivo samples.zip.



Em segundo lugar, nós descompactamos a pasta.



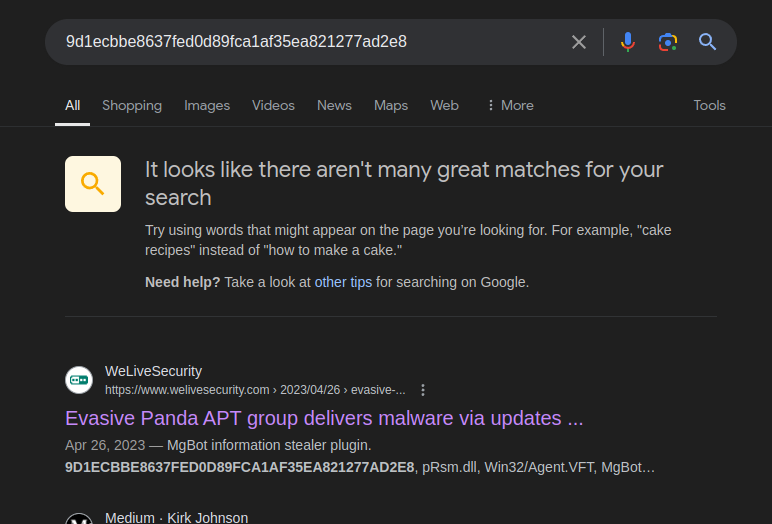
Por fim, nós geramos o hash SHA1 do arquivo desejado utilizando a ferramenta sha1sum do Linux.



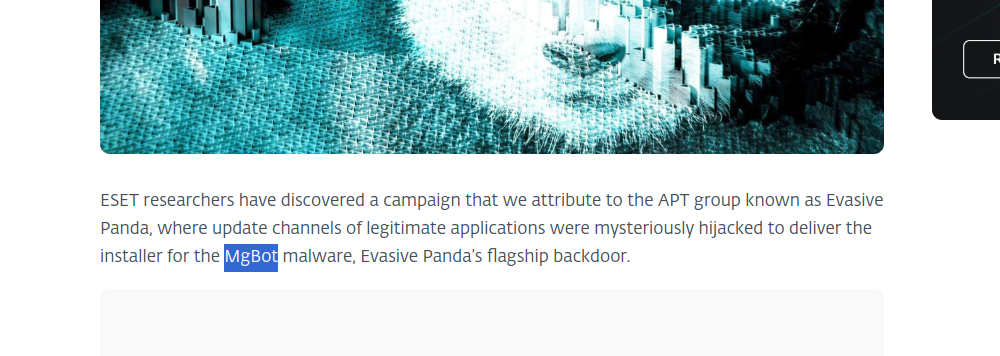
R: 9d1ecbbe8637fed0d89fca1af35ea821277ad2e8.

**Which malware framewOrk utilizes these DLLs as add-on modules?**

Para responder essa pergunta, buscou-se no navegador o hash encontrado na questão anterior com o objetivo de procurar referências para o arquivo de malware.



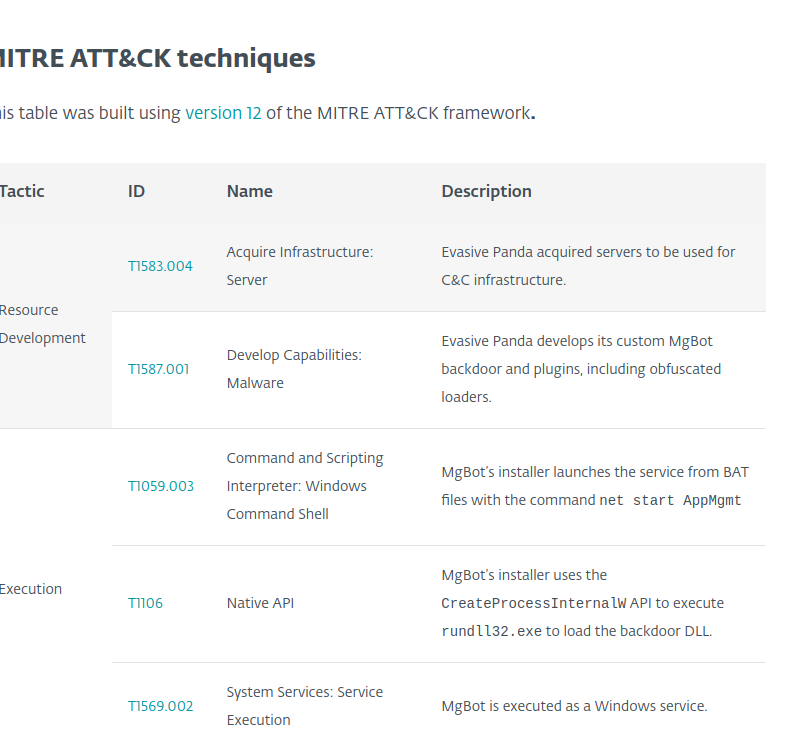
O site *WeLiveSecurity* postou um artigo, que será ainda muito usado nessa sala, a respeito do malware. Ref: [https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/.](https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/)

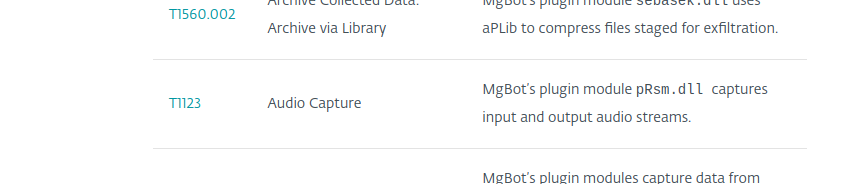


R: MgBot.

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

No próprio artigo encontram-se referências para as técnicas do MITRE que podem ser linkadas ao ataque.





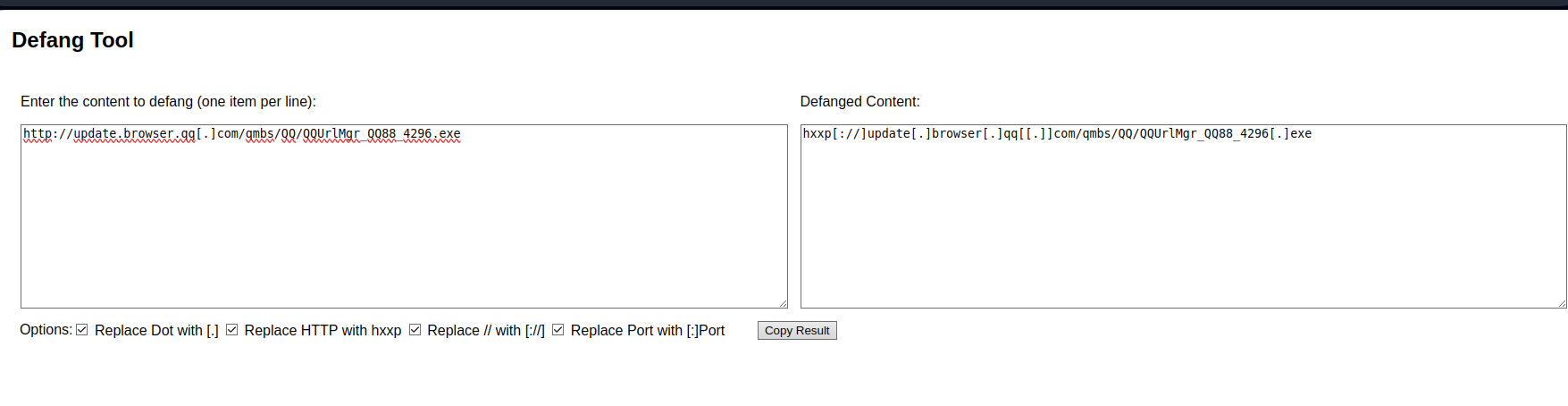
R: T1123.

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

Novamente, o artigo fornece a informação da URL que o arquivo malicioso apareceu no ano da questão.



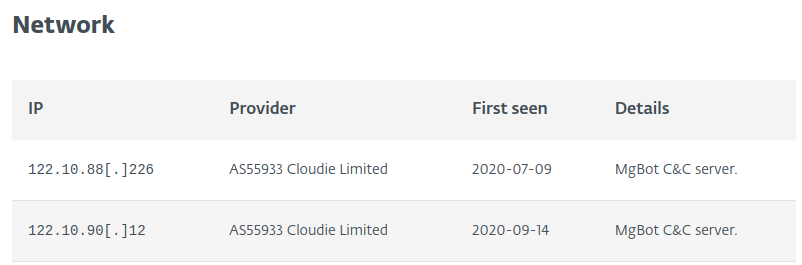
O link em questão não está totalmente no formato de Defang (desativado), usamos então o site defa.ng para completar. Ref: [https://defa.ng](https://defa.ng/).



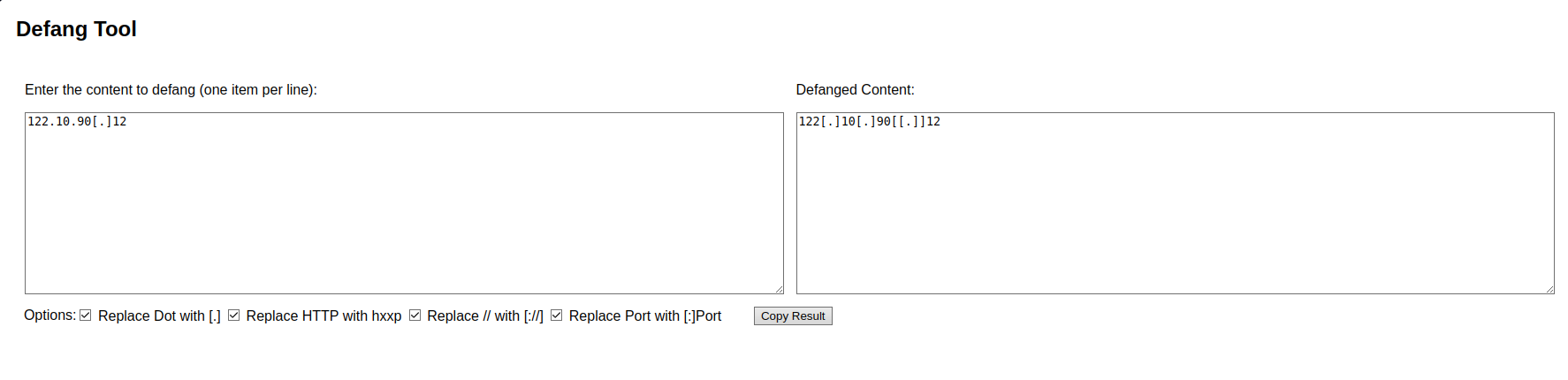
R: hxxp[://]update[.]browser[.]qq[.]com/qmbs/QQ/QQUrlMgr\_QQ88\_4296[.]exe.

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

Essa informação está contida na parte de "Network" da página estudada ao longo dessa sala.



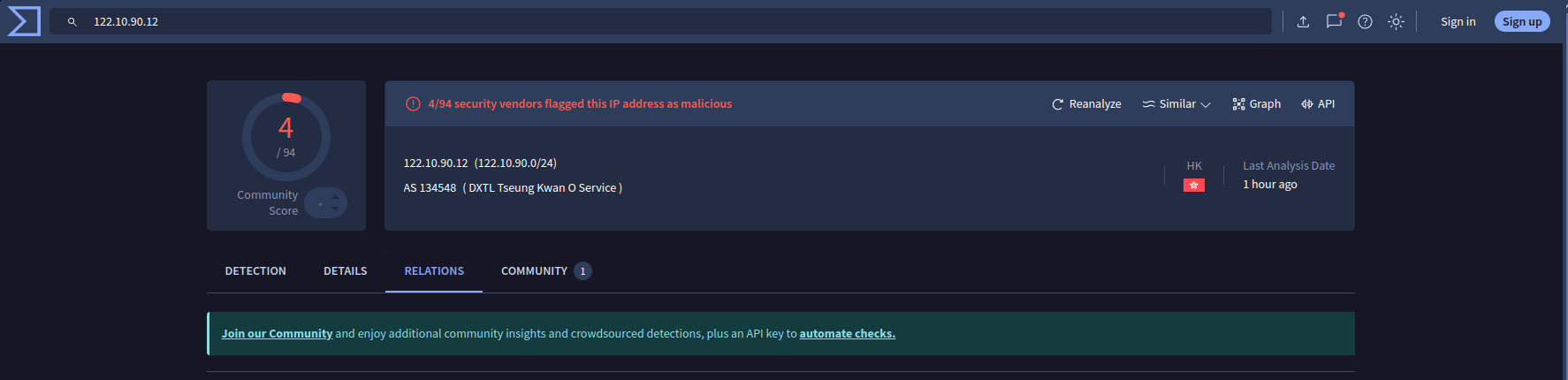
Novamente, é necessário completar o Defang desse IP. Novamente, vamos usar o defa.ng para fazer o processo.



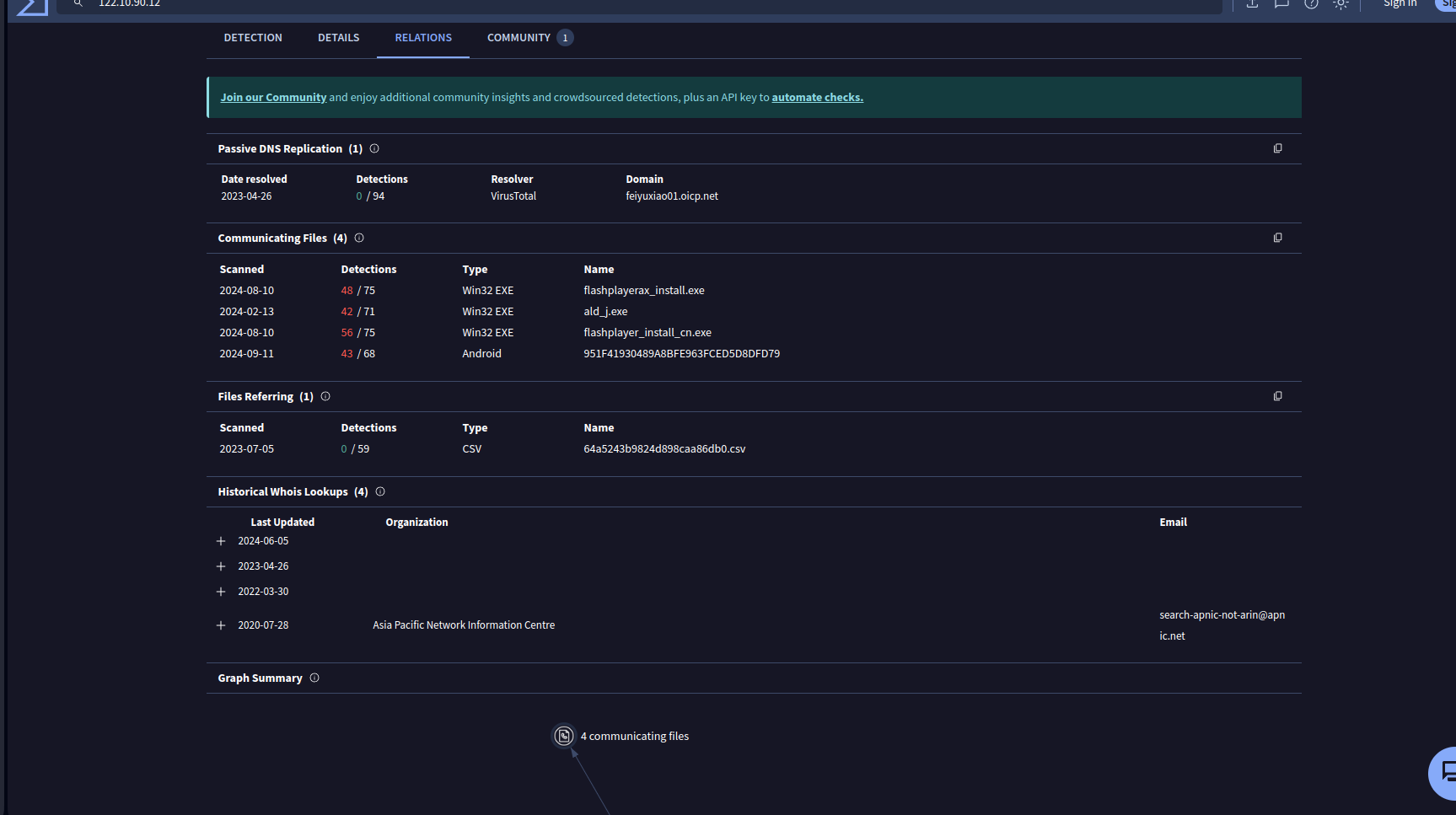
R: 122[.]10[.]90[.]12.

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

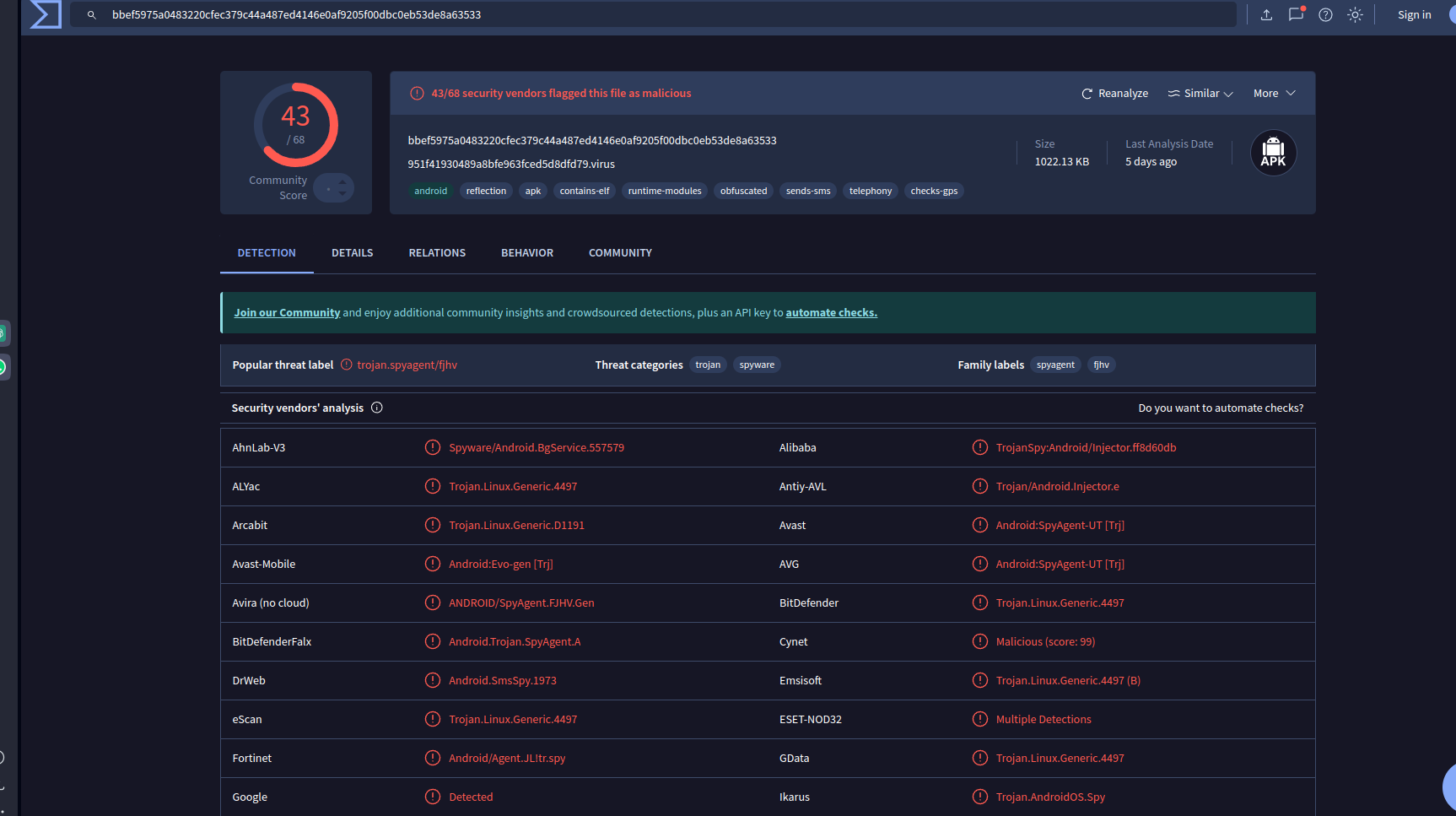
Inicialmente, devemos jogar o IP que encontramos para a data específicada no VirusTotal. Ref: https://virustotal.com.



Na aba de relations encontramos o arquivo Android que o enunciado busca.



Clicando no arquivo, nós agora podemos encontrar o hash SHA1 dele.



R: 1c1fe906e822012f6235fcc53f601d006d15d7be

**Conclusão**

Este CTF oferece uma experiência prática de nível fácil, ideal para iniciantes na área de Blue Team e inteligência de ameaças cibernéticas. Ao final, os participantes compreendem melhor uma parcela de trabalho de um analista SOC.

**Referências**

* [https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/.](https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/)
* [https://defa.ng](https://defa.ng/).
* [https://virustotal.com](https://virustotal.com/).