TryHackMe: Masterminds

16:20

AVISO: NÃO INTERAJA COM NENHUM DOMÍNIO OU ENDEREÇO IP DESTE CTF!!!

Infecção 1

Abra o arquivo pcap e comece a investigação.

Antes de tudo, vamos selecionar o “Activity Overview” para ver uma visão geral do que está contido neste pcap.

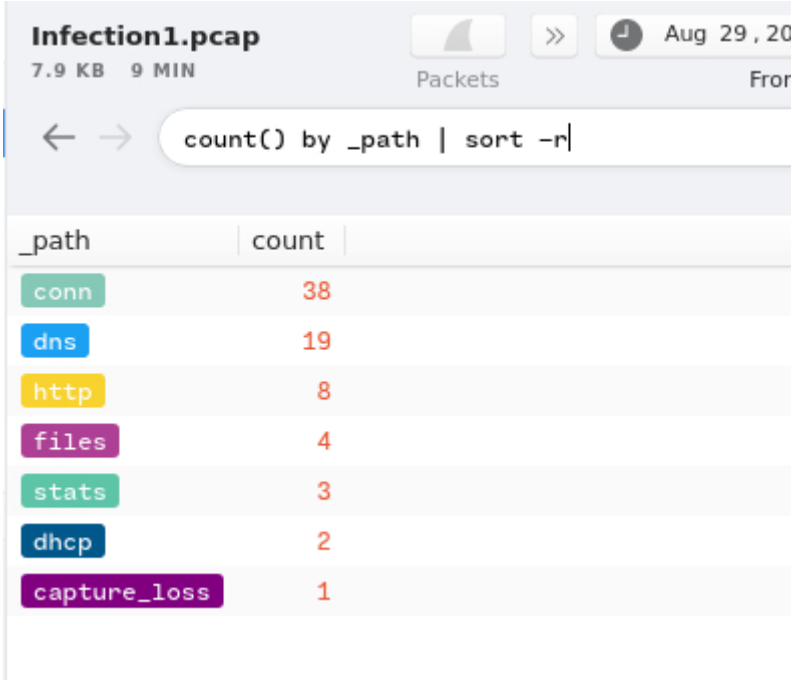


Figura 1 - Activity Overview do primeiro arquivo.

Vamos manter esses dados em mente para nossas próximas análises.

Providencie o endereço IP da vítima.

Podemos utilizar uma das buscas já prontas do Brim para descobrir as ameaças, com o “Suricata Alerts by Category”.

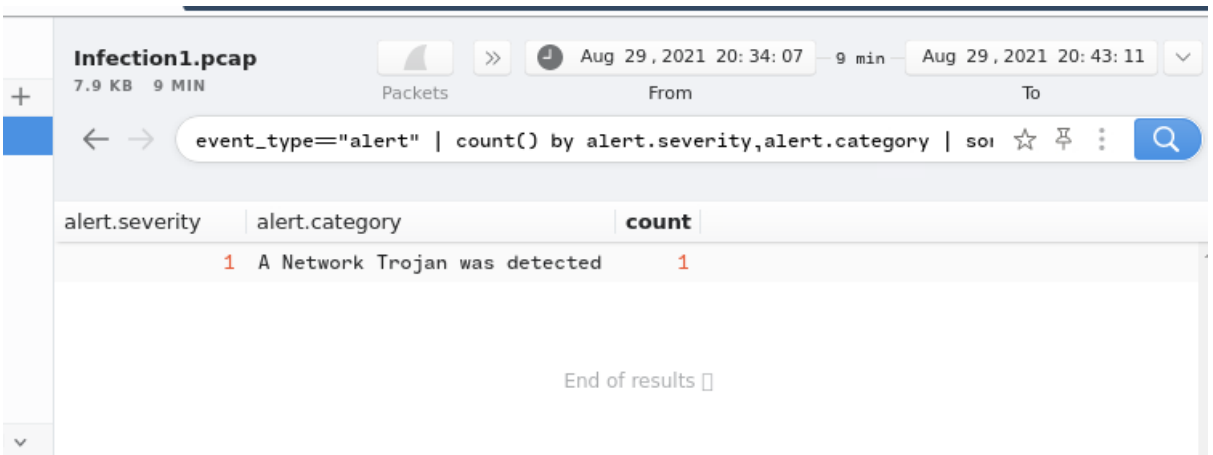


Figura 2 - Alertas do Suricata do primeiro arquivo.

Parece que só existe um alerta. Vamos filtrar os resultados para encontrar mais dados sobre este alerta, e possivelmente encontraremos o endereço de IP desejado.

Comando 1: `alert.category == "A Network Trojan was detected"`

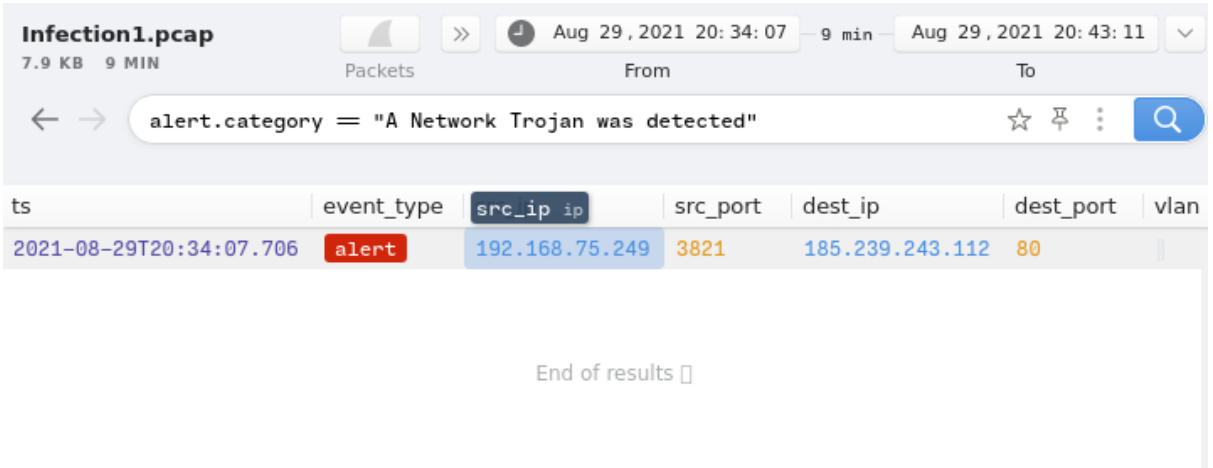


Figura 3 - Retorno do Comando 1.

R: 192.168.75.249

A vítima tentou fazer conexões HTTP para dois domínios suspeitos com o status de '404 not found'. Providencie esses hosts/domínios.

Isso também pode se resolver de forma fácil, pois só existem 8 logs de conexão HTTP. Vamos fazer uma busca nesses logs e receber somente o host e a mensagem de status.

Comando 2: `_path=="http" | cut host,status_msg`

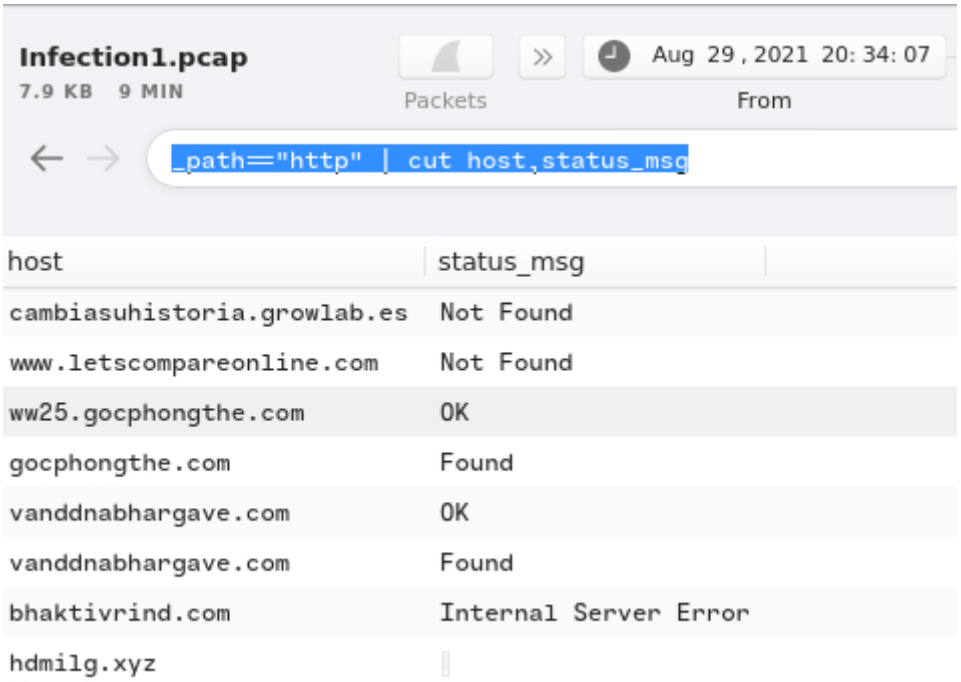


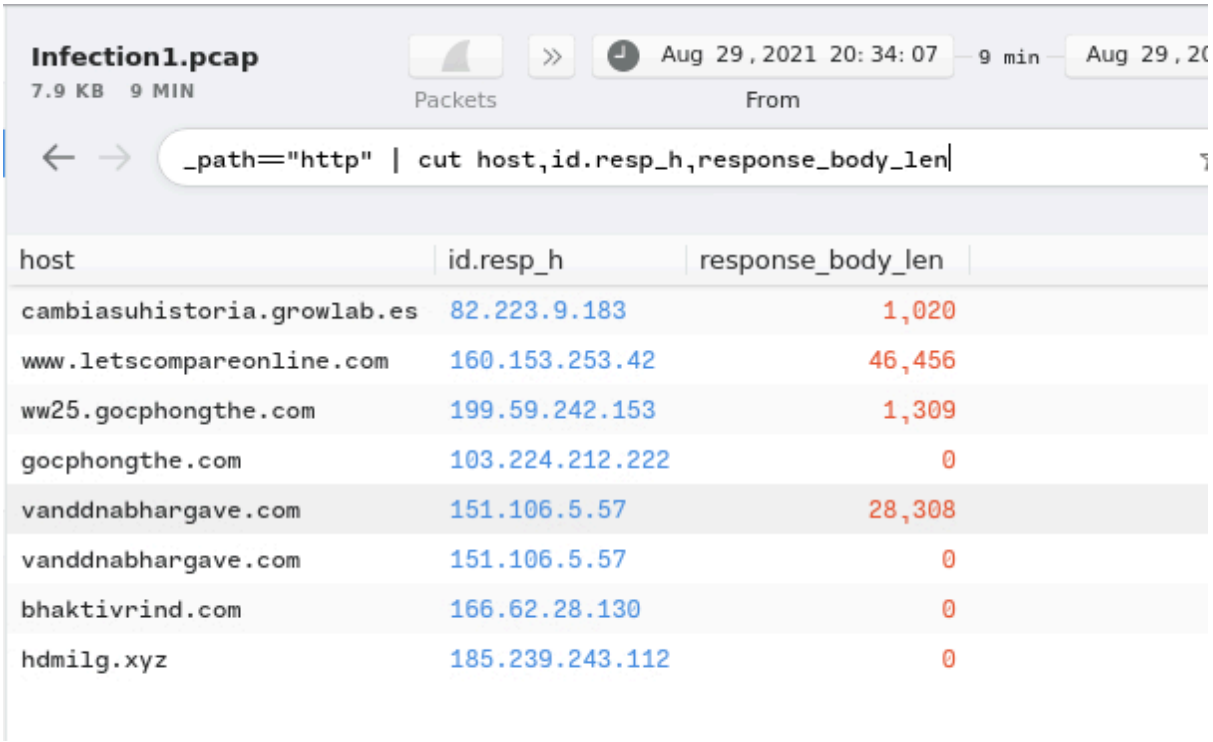
Figura 4 - Retorno do Comando 2.

R: cambiasuhistoria.growlab.es,www.letscompareonline.com

A vítima fez uma conexão HTTP bem sucedida com um dos domínios, e recebeu um response_body_len de 1,309. Providencie o domínio e o endereço de IP destinatário.

Fazendo uma pequena mudança no Comando 2, podemos mudar os parâmetros para observar somente o que a questão deseja.

Comando 3: `_path=="http" | cut host,id.resp_h,response_body_len`



host	id.resp_h	response_body_len
cambiasuhistoria.growlab.es	82.223.9.183	1,020
www.letscompareonline.com	160.153.253.42	46,456
ww25.gocphongthe.com	199.59.242.153	1,309
gocphongthe.com	103.224.212.222	0
vanddnabhargave.com	151.106.5.57	28,308
vanddnabhargave.com	151.106.5.57	0
bhaktivrind.com	166.62.28.130	0
hdmilg.xyz	185.239.243.112	0

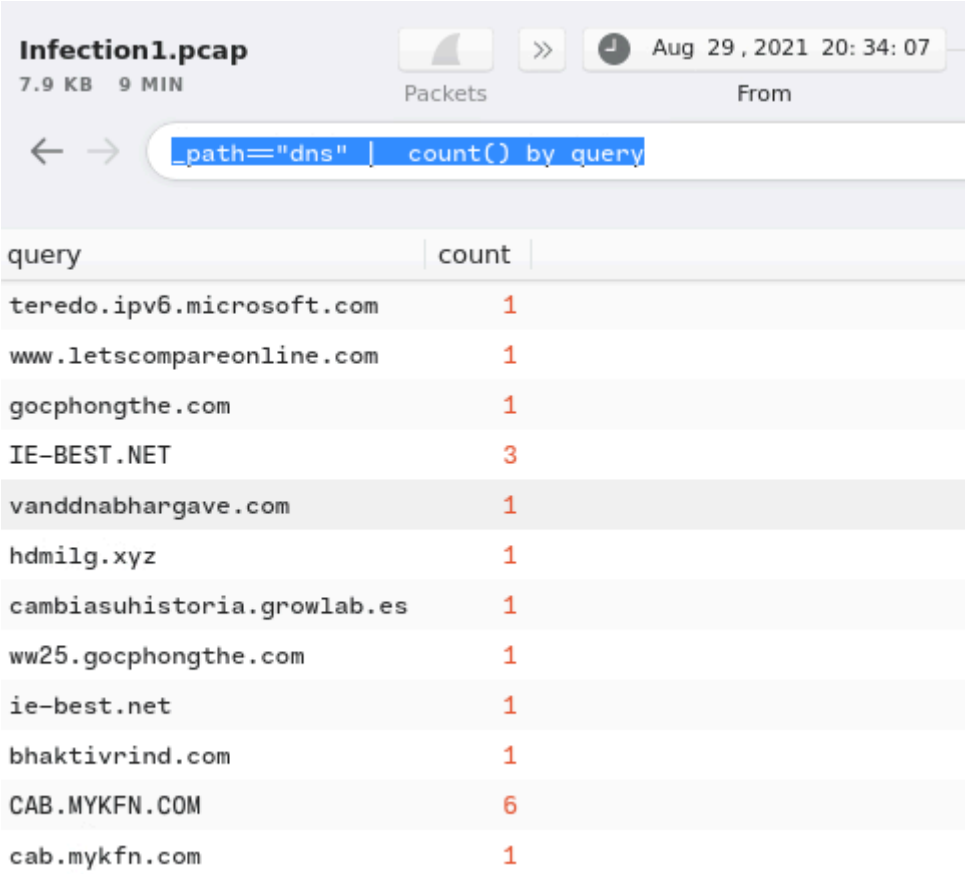
Figura 5 - Retorno do Comando 3.

R: ww25.gocphongthe.com,199.59.242.153

Quantos pedidos únicos de DNS foram feitos para o domínio cab[.]myfkn[.]com (incluindo o domínio em CAPS)?

Agora estamos procurando somente nos pedidos DNS, e seria mais apropriado realizar uma contagem dos domínios no caminho DNS.

Comando 4: `_path=="dns" | count() by query`



query	count
teredo.ipv6.microsoft.com	1
www.letscompareonline.com	1
gocphongthe.com	1
IE-BEST.NET	3
vanddnabhargave.com	1
hdmilg.xyz	1
cambiasuhistoria.growlab.es	1
ww25.gocphongthe.com	1
ie-best.net	1
bhaktivrind.com	1
CAB.MYKFN.COM	6
cab.mykfn.com	1

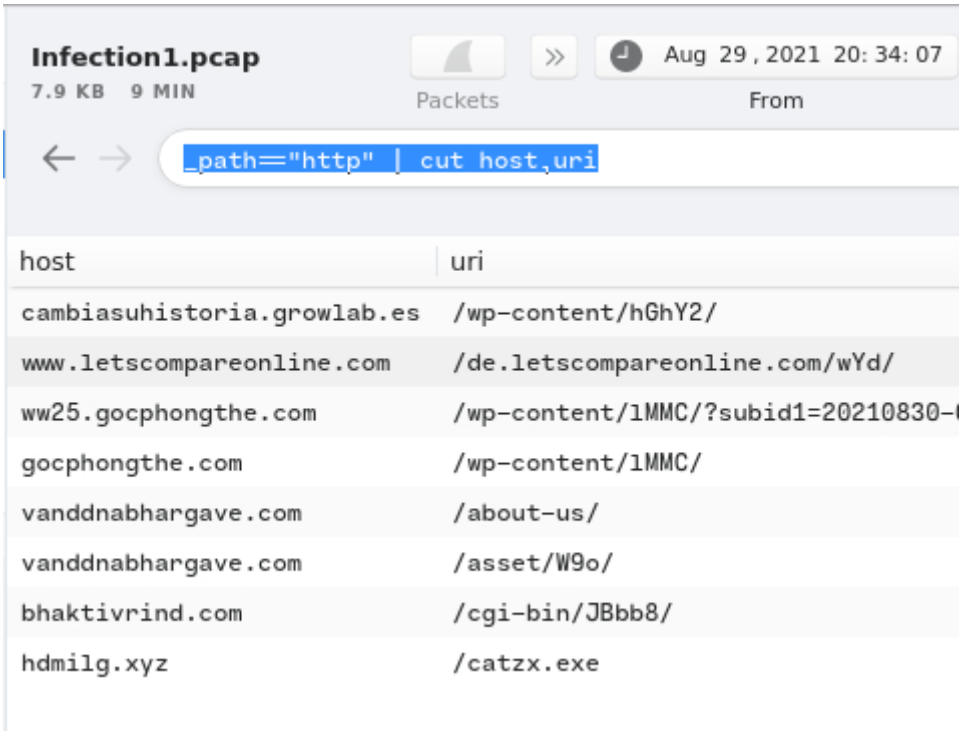
Figura 6 - Retorno do Comando 4.

R: 7

Providencie o URI do domínio bhaktivrind[.]com que a vítima contatou por HTTP.

Novamente, tudo que é necessário é colocar os parâmetros de busca apropriados para encontrar a resposta.

Comando 5: `_path=="http" | cut host,uri`



host	uri
cambiasuhistoria.growlab.es	/wp-content/hGhY2/
www.letscompareonline.com	/de.letscompareonline.com/wYd/
ww25.gocphongthe.com	/wp-content/1MMC/?subid1=20210830-
gocphongthe.com	/wp-content/1MMC/
vanddnabhargave.com	/about-us/
vanddnabhargave.com	/asset/W9o/
bhaktivrind.com	/cgi-bin/JBbb8/
hdmilg.xyz	/catzx.exe

Figura 7 - Retorno do Comando 5.

R: /cgi-bin/JBbb8/

Providencie o endereço IP do servidor malicioso e o executável que a vítima baixou do servidor.

É possível ver na Figura 3 que o endereço de IP que causou o alerta é o 185.239.243.112, e na Figura 7 um URI suspeito com um executável. Realizando uma rápida busca, é possível descobrir que nossa suspeita estava correta, pois esse URI veio do IP suspeito.

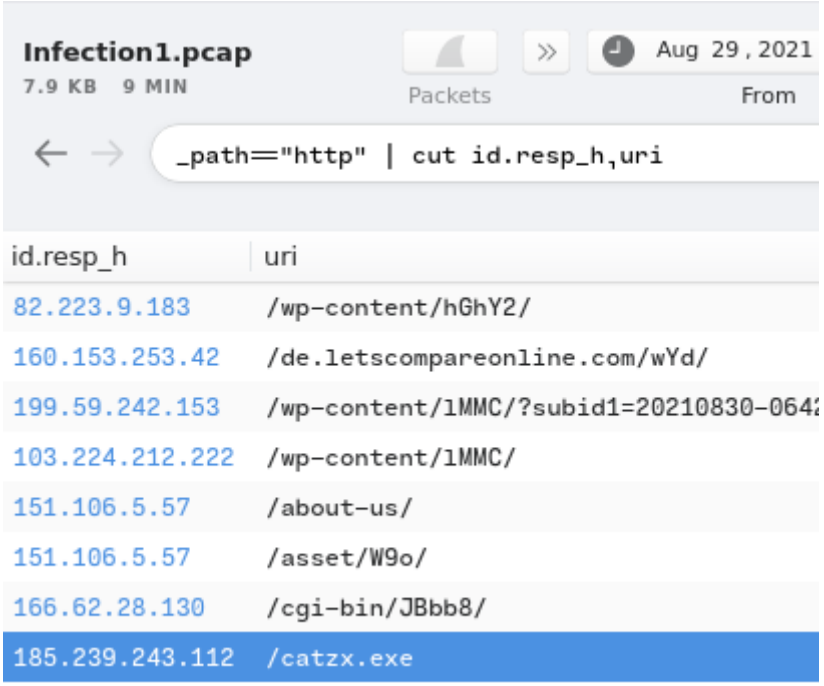


Figura 8 - Pesquisa com filtro de IP de destino e URI.

R: 185.239.243.112,catzx.exe

Baseado na informação coletada na segunda questão providencie o nome do malware usando o VirusTotal.

Recapitulando, os dois domínios encontrados na segunda questão são: cambiasuhistoria.growlab.es e www.letscompareonline.com, e, analisando os dois links, temos resultados bem parecidos, mas o interessante se encontra na aba “Community”.

Figura 9 - Recorte da pesquisa no VirusTotal.

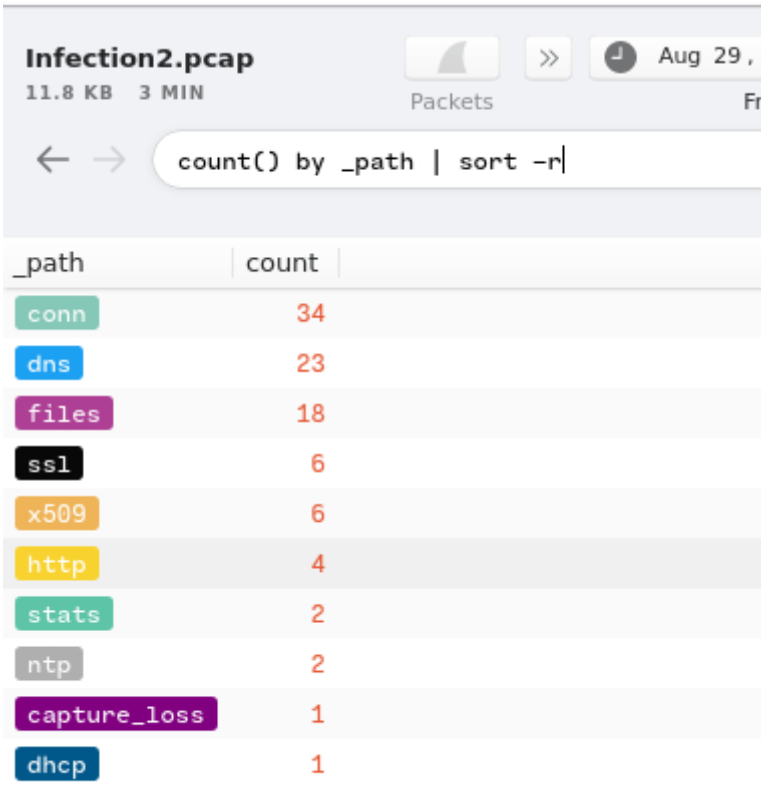
Traduzindo, um IOC (Indicador de Comprometimento) é usado para descrever o que causou o ataque. Podemos ver que os dois pastebins falam sobre IOCs da Emotet, o que pode nos indicar que Emotet é o malware comprometedor.

R: Emotet

Infecção 2

Abra o arquivo pcap e comece a investigação.

Novamente, vamos olhar o “Activity Overview” para obtermos uma visão geral dos eventos.



_path	count
conn	34
dns	23
files	18
ssl	6
x509	6
http	4
stats	2
ntp	2
capture_loss	1
dhcp	1

Figura 10 - Activity Overview do segundo arquivo.

Providencie o endereço IP da máquina da vítima.

Assim como na infecção anterior, vamos olhar as categorias de ameaça do Suricata para ver o que aconteceu.

Infection2.pcap
11.8 KB 3 MIN
Packets
Aug 29, 2021 20:19:28
From

```
event_type=="alert" | count() by alert.severity,alert.
```

alert.severity	alert.category	count
2	Potentially Bad Traffic	2
1	A Network Trojan was detected	2

Figura 11 - Alertas do Suricata do segundo arquivo.

A mesma categoria novamente. Vamos fazer uso do Comando 1 novamente para achar o endereço IP da vítima.

Infection2.pcap
11.8 KB 3 MIN
Packets
Aug 29, 2021 20:19:28 — 3 min — Aug 29, 2021 20:22
From
To

```
alert.category == "A Network Trojan was detected"
```

ts	event_type	src_ip	src_port	dest_ip	dest_port
2021-08-29T20:20:01.932	alert	192.168.75.146	1046	45.95.203.28	80
2021-08-29T20:20:01.932	alert	192.168.75.146	1046	45.95.203.28	80

Figura 12 - Retorno do Comando 1 no segundo arquivo.

R: 192.168.75.146

Providencie o endereço IP com o qual a vítima fez conexões POST.

A busca pré-pronta do Brim “HTTP Post Requests” pode nos ajudar neste exercício. Ao utilizá-la, é possível ver que só tem 3 resultados e os 3 são direcionados ao mesmo endereço IP de destino, então podemos assumir que esta é a nossa resposta.

11.8 KB 3 MIN
Packets
From

```
method=="POST" | cut ts, uid, id, method, uri, status_code
```

	id.orig_h	id.orig_p	id.resp_h	id.resp_p	method
sW81BjTY3DopW82	192.168.75.146	1052	5.181.156.252	80	POST
cvDakTgZKvwvxi	192.168.75.146	1048	5.181.156.252	80	POST
GDy2Q3cq1f0q3C8	192.168.75.146	1047	5.181.156.252	80	POST

Figura 13 - Pedidos HTTP com o método POST no segundo arquivo.

R: 5.181.156.252

Quantas conexões POST foram feitas para o IP destinatário da questão anterior?

R: 3

Providencie o domínio do qual o binário foi baixado.

Como só temos 4 pedidos HTTP, podemos usar a busca do Brim “HTTP Requests” e provavelmente acharemos a resposta.

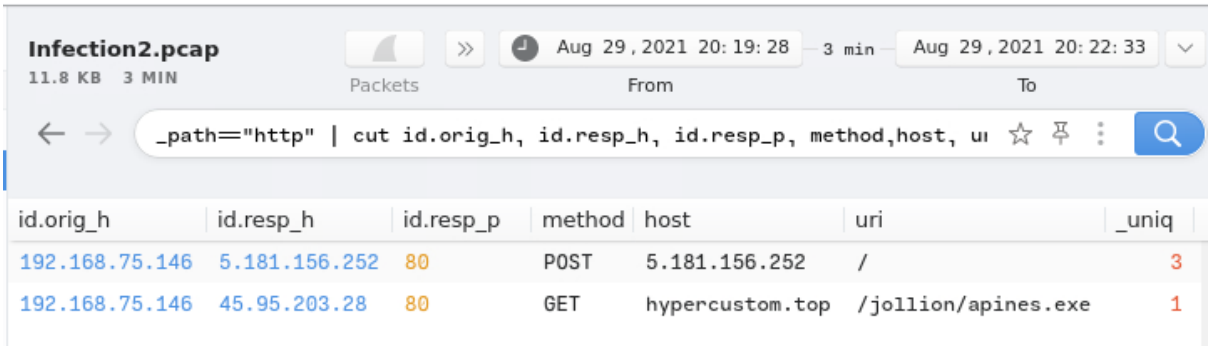


Figura 14 - Pedidos HTTP com qualquer método no segundo arquivo.

R: hypercustom.top

Providencie o nome do binário, incluindo o URI completo.

R: /jollion/apines.exe

Providencie o endereço IP do domínio que hospeda o binário.

R: 45.95.203.28

Tinham 2 alertas Suricata de “A Network Trojan was detected”. Qual eram os endereços IP de origem e destino?

Essa informação já está contida na Figura 11.

R: 192.168.75.146,45.95.203.28

Olhando o domínio .top nos pedidos HTTP, providencie o nome do ladrão envolvido nesse pacote usando o banco de dados URLhaus.

https://urlhaus.abuse.ch/

Pesquisando o hypercustom.top no banco de dados, podemos achar a resposta rapidamente.

Browse Database

domain, url, md5, sha256, tag:SocGholish, filetype:doc or url_status:online

Search

URLs | Payloads

Dateadded (UTC)	Malware URL	Status	Tags	Reporter
2021-08-21 19:44:08	http://hypercustom.top/jollion/apines.exe	Offline	cryptbot exe opendir RedLineStealer	abuse_ch
2021-08-19 19:47:07	http://hypercustom.top/jollion/apines1.exe	Offline	32 exe opendir RedLineStealer	zbetcheckin
2021-08-19 19:02:05	http://hypercustom.top/jollion/lipster.exe	Offline	32 exe opendir RedLineStealer	zbetcheckin
2021-08-19 18:57:06	http://hypercustom.top/holler/rollerkind2.exe	Offline	32 exe RedLineStealer	zbetcheckin
2021-08-19 18:57:06	http://hypercustom.top/holler/rollerkind.exe	Offline	32 exe RedLineStealer	zbetcheckin

Previous Next

Figura 15 - Recorte da pesquisa no URLhaus.

R: RedLine Stealer

Infecção 3

Abra o arquivo pcap e comece a investigação.

Pela última vez na atividade, vamos olhar o “Activity Overview” para obtermos uma visão geral dos eventos.

Infection3.pcapng
296.4 KB 11 MIN

Packets | Aug 29, 2021 00:25:31 From

```
count() by _path | sort -r
```

_path	count
dns	986
conn	914
files	574
ssl	331
x509	200
ntlm	40
http	25
notice	11
dhcp	8
stats	4
weird	3
capture_loss	1

Figura 16 - Activity Overview do terceiro arquivo.

É perceptível que tem muito mais eventos nesta infecção, então uma filtragem mais acurada será necessária.

Providencie o endereço IP da máquina da vítima.

Vamos olhar as categorias de ameaça do Suricata para fazer a análise.

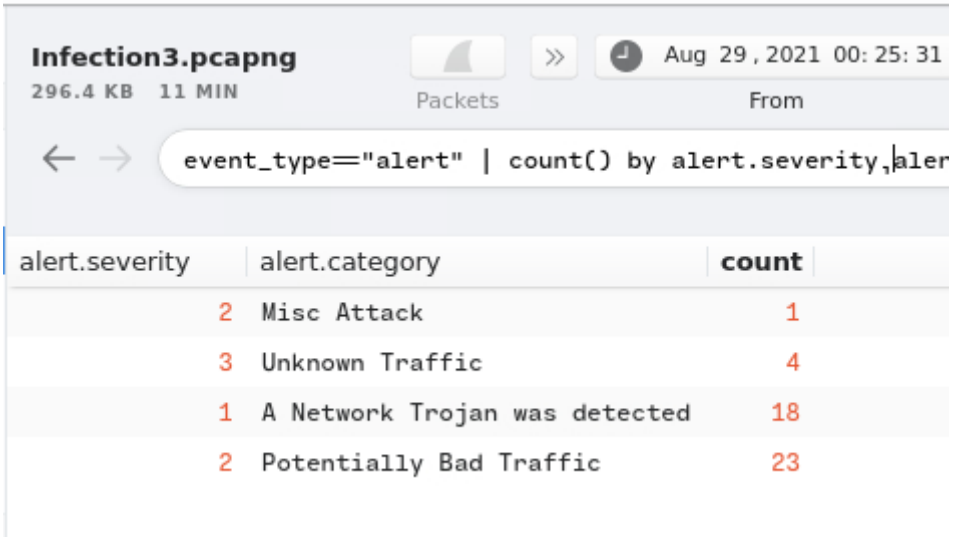


Figura 17 - Alertas do Suricata do terceiro arquivo.

Duas categorias chamam atenção, “A Network Trojan was detected” e “Misc Attack”, então devemos fazer o filtro por qualquer uma dessas ocorrências.

Comando 6: `alert.category == "A Network Trojan was detected" or "Misc Attack"`

Infection3.pcapng
296.4 KB 11 MIN

Packets | Aug 29, 2021 00:25:31 From | 11 min | Aug 29, 2021 00:37:11 To

alert.category == "A Network Trojan was detected" or "Misc Attack"

	event_type	src_ip	src_port	dest_ip	dest_port	vlan	pr
21-08-29T00:36:23.204	alert	192.168.75.232	54451	63.251.106.25	80		T
21-08-29T00:35:49.022	alert	192.168.75.232	56974	63.251.106.25	80		T
21-08-29T00:35:16.227	alert	192.168.75.232	56973	63.251.106.25	80		T
21-08-29T00:34:43.431	alert	192.168.75.232	56972	63.251.106.25	80		T
21-08-29T00:34:10.602	alert	192.168.75.232	56971	63.251.106.25	80		T
21-08-29T00:33:31.071	alert	192.168.75.232	56970	199.21.76.77	80		T
21-08-29T00:32:58.386	alert	192.168.75.232	56969	199.21.76.77	80		T
21-08-29T00:32:25.665	alert	192.168.75.232	56968	199.21.76.77	80		T
21-08-29T00:31:52.964	alert	192.168.75.232	56967	199.21.76.77	80		T
21-08-29T00:31:20.274	alert	192.168.75.232	56965	199.21.76.77	80		T
21-08-29T00:30:47.071	alert	192.168.75.232	56961	162.217.98.146	80		T
21-08-29T00:30:14.417	alert	192.168.75.232	56958	162.217.98.146	80		T
21-08-29T00:29:41.723	alert	192.168.75.232	56954	162.217.98.146	80		T
21-08-29T00:29:08.995	alert	192.168.75.232	56951	162.217.98.146	80		T
21-08-29T00:28:36.323	alert	192.168.75.232	56950	162.217.98.146	80		T
21-08-29T00:26:09.087	alert	63.251.106.25	80	192.168.75.232	56927		T
21-08-29T00:26:07.279	alert	199.21.76.77	80	192.168.75.232	56926		T
21-08-29T00:26:05.871	alert	162.217.98.146	80	192.168.75.232	56925		T
21-08-29T00:26:05.005	alert	92.63.197.153	80	192.168.75.232	56924		T

Figura 18 - Retorno do Comando 6.

Podemos ver que o endereço 192.168.75.232 está presente em todas as comunicações, e sempre iniciando ou recebendo uma conexão com endereços IP na porta 80 (HTTP), portanto é razoável assumir que essa é a vítima.

R: 192.168.75.232

Providencie 3 domínios C2 dos quais binários foram baixados(do evento mais velho ao mais novo).

Pelo grande número de pedidos HTTP, isso será um pouco mais difícil. Vamos filtrar pelos conteúdos host e uri para olharmos somente o que importa.

Comando 7: `_path=="http" | count() by host,uri`

Infection3.pcapng
296.4 KB 11 MIN

Packets | Aug 29, 2021 00:25:31 | 11 min | From

```
_path=="http" | count() by host,uri
```

host	uri
xfhoahegue.ru	/s/5.exe
afhoahegue.ru	/s/3.exe
tile-service.weather.microsoft.com	/en-US/livetile/preinstall?region=US&a
efhoahegue.ru	/s/4.exe
efhoahegue.ru	/s/2.exe
efhoahegue.ru	/s/1.exe
x1.i.lencr.org	/
xfhoahegue.ru	/s/4.exe
xfhoahegue.ru	/s/2.exe
xfhoahegue.ru	/s/1.exe
efhoahegue.ru	/s/5.exe
xfhoahegue.ru	/s/VNEW=1
afhoahegue.ru	/s/4.exe
afhoahegue.ru	/s/2.exe
afhoahegue.ru	/s/1.exe
efhoahegue.ru	/s/3.exe
afhoahegue.ru	/s/VNEW=1
xfhoahegue.ru	/s/3.exe
afhoahegue.ru	/s/5.exe
ctldl.windowsupdate.com	/msdownload/update/v3/static/trustedr/
ctldl.windowsupdate.com	/msdownload/update/v3/static/trustedr/

Figura 19 - Retorno do Comando 7.

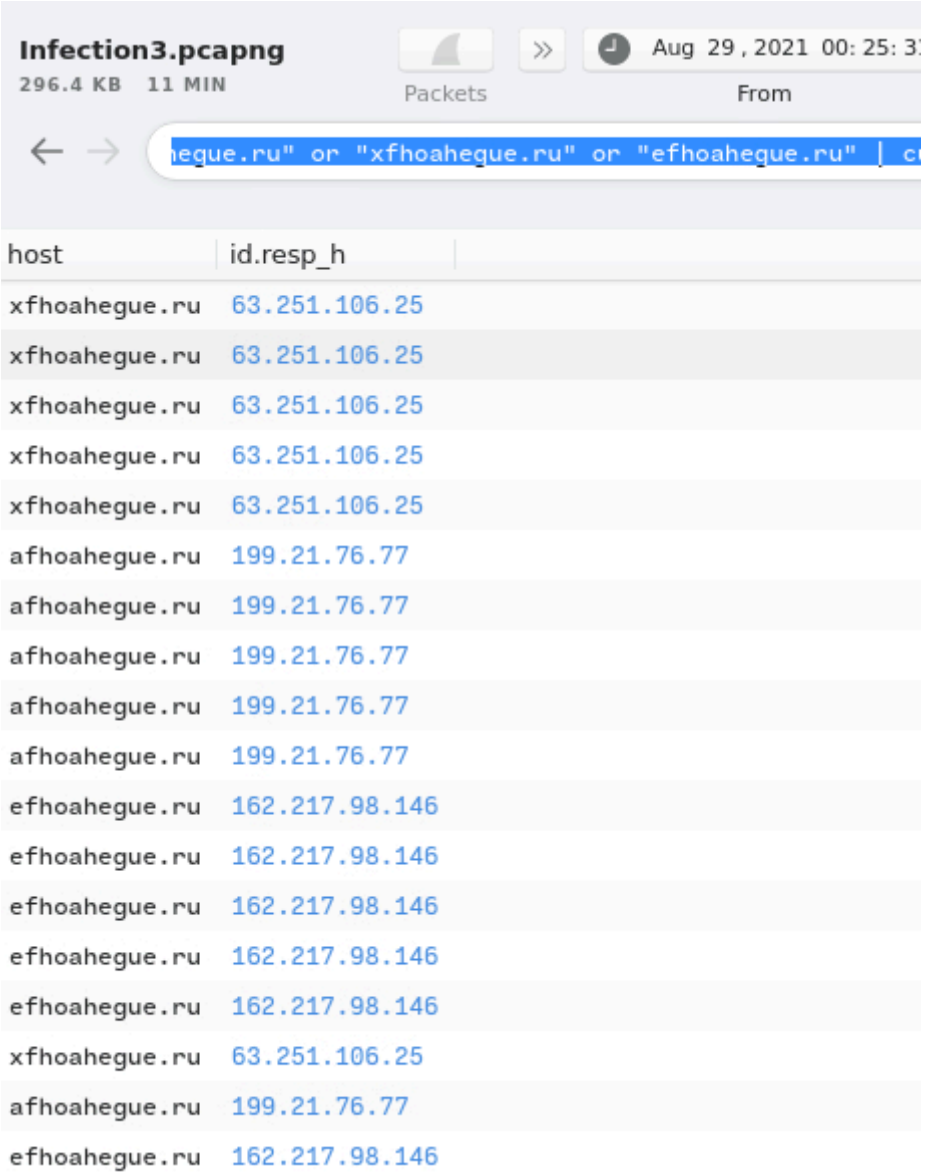
Olhando os resultados, temos só 3 domínios dos quais 5 binários diferentes estão sendo baixados, e eles são nossas respostas:

R: efhoahegue.ru,afhoahegue.ru,xfhoahegue.ru

Providencie os endereços IP dos 3 domínios na questão anterior.

Vamos pegar somente os eventos com os hosts iguais a questão anterior e exibir somente o host e o IP de destino.

Comando 8: `_path=="http" | host=="afhoahegue.ru" or "xfhoahegue.ru" or "efhoahegue.ru" | cut host,id.resp_h`



host	id.resp_h
xfhoahegue.ru	63.251.106.25
xfhoahegue.ru	63.251.106.25
xfhoahegue.ru	63.251.106.25
xfhoahegue.ru	63.251.106.25
xfhoahegue.ru	63.251.106.25
afhoahegue.ru	199.21.76.77
afhoahegue.ru	199.21.76.77
afhoahegue.ru	199.21.76.77
afhoahegue.ru	199.21.76.77
afhoahegue.ru	199.21.76.77
efhoahegue.ru	162.217.98.146
efhoahegue.ru	162.217.98.146
efhoahegue.ru	162.217.98.146
efhoahegue.ru	162.217.98.146
efhoahegue.ru	162.217.98.146
xfhoahegue.ru	63.251.106.25
afhoahegue.ru	199.21.76.77
efhoahegue.ru	162.217.98.146

Figura 20 - Retorno do Comando 8.

R: 162.217.98.146,199.21.76.77,63.251.106.25

Quantas buscas DNS únicas foram feitas para o domínio associado ao primeiro endereço de IP da última questão?

Podemos achar essa resposta filtrando o campo query dos pedidos DNS que tem o valor "efhoahegue.ru"

Comando 9: `_path=="dns" | query=="efhoahegue.ru" | count() by query`

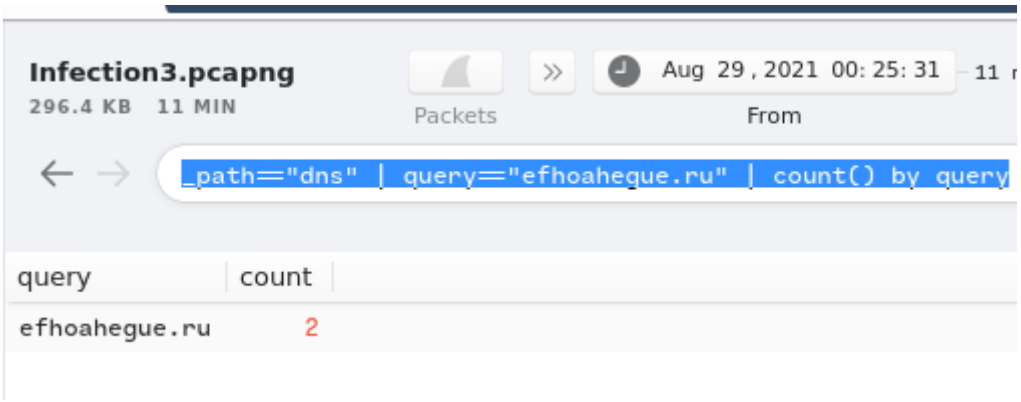


Figura 21 - Retorno do Comando 9.

R: 2

Quantos binários foram baixados do domínio da questão anterior no total?

Podemos fazer uma busca nos pedidos HTTP com o hosy “efhoahegue.ru” e filtrar o host e o uri para obter essa resposta.

Comando 10: `_path=="http" | host=="efhoahegue.ru" | cut host,uri`

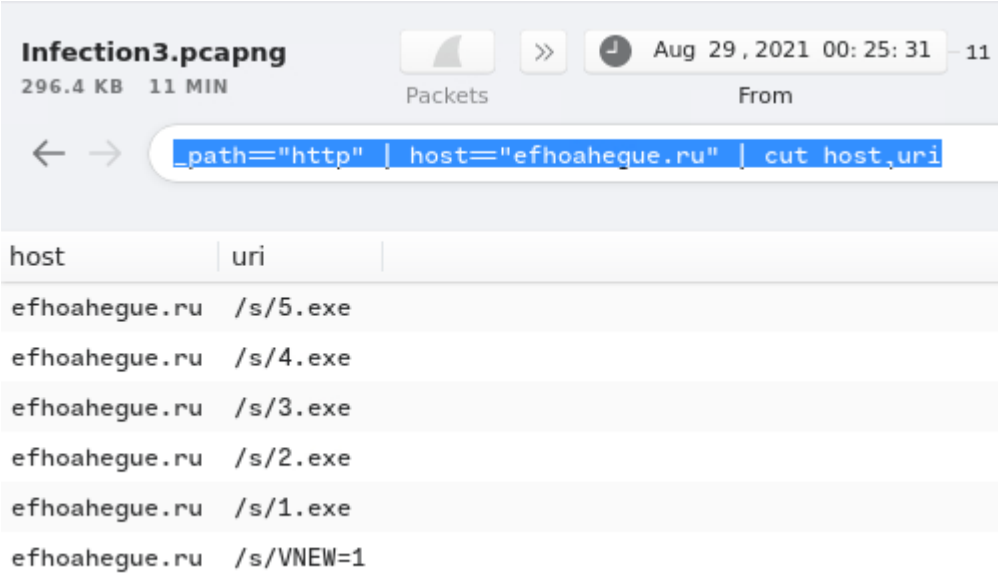


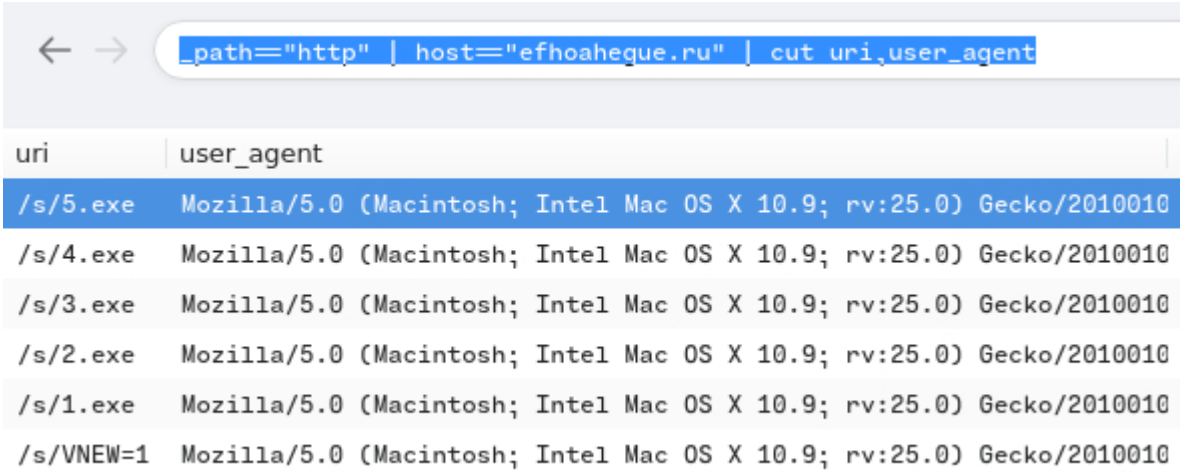
Figura 22 - Retorno do Comando 10.

R: 5

Providencie o agente de usuário usado para realizar o download dos binários.

Com uma simples mudança no Comando 10, podemos encontrar essa resposta.

Comando 11: `_path=="http" | host=="efhoahegue.ru" | cut uri,user_agent`



_path=="http" | host=="efhoahegue.ru" | cut uri,user_agent

uri	user_agent
/s/5.exe	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/2010010
/s/4.exe	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/2010010
/s/3.exe	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/2010010
/s/2.exe	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/2010010
/s/1.exe	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/2010010
/s/VNEW=1	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/2010010

Figura 23 - Retorno do Comando 11.

R: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.9; rv:25.0) Gecko/20100101 Firefox/25.0

Providencie a quantidade de conexões DNS feitas nessa captura de pacote.

Podemos achar a resposta na Figura 16.

R: 986

Com suas habilidades de OSINT, providencie o nome da worm usando o primeiro domínio coletado na questão 2 (Por favor use aspas em suas pesquisas google, não coloque .ru na sua pesquisa, e NÃO interaja com o domínio diretamente)

Uma rápida pesquisa no google seguindo as recomendações do exercício resolve o problema.

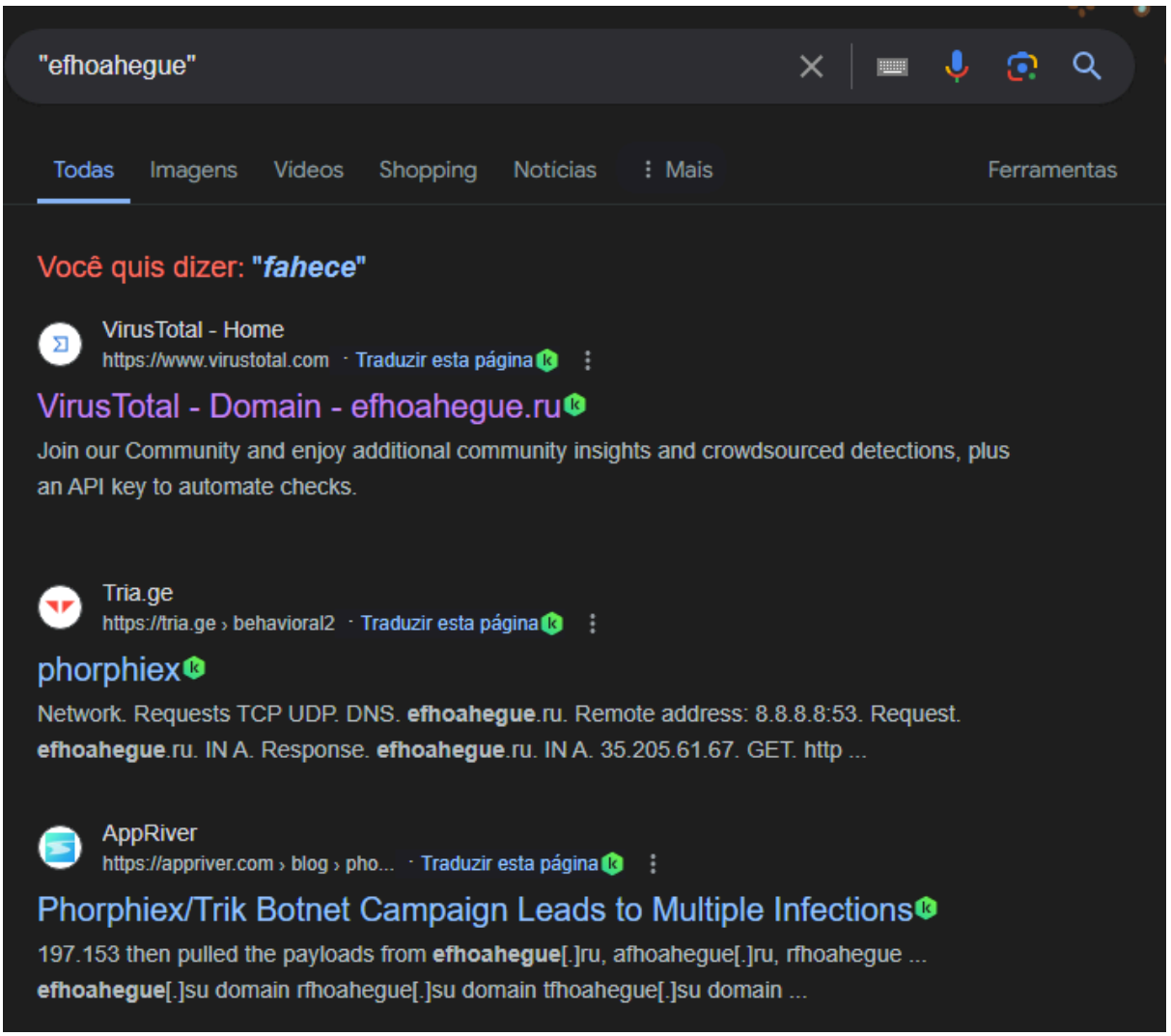


Figura 24 - Recorte da pesquisa no Google.

R: Phorphiex