Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Carnage – TryHackme

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Carnage – Sérgio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 24/10/2024 |
| **Link** | <https://tryhackme.com/r/room/c2carnage> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Sérgio Guidi Trovo | Estudante |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | DD/MM/AAAA | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

Sumário

[Contextualização 3](#_Toc180675017)

[Desenvolvimento 3](#_Toc180675018)

[Pergunta 1 - What was the date and time for the first HTTP connection to the malicious IP? 4](#_Toc180675019)

[Pergunta 2 - Wha tis the name of the zip file that was downloaded? 5](#_Toc180675020)

[Pergunta 3 - What was the domain hosting the malicious zip file? 6](#_Toc180675021)

[Pergunta 4 - Without downloading the file, what is the name of the file in the zip file? 6](#_Toc180675022)

[Pergunta 5 - What is the name of the webserver of the malicious IP from which the zip file was downloaded? 7](#_Toc180675023)

[Pergunta 6 - What is the version of the webserver from the previous question? 8](#_Toc180675024)

[Pergunta 7 - Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity? 8](#_Toc180675025)

[Pergunta 8 - Which certificate authority issued the SSL certificate to the first domain from the previous question? 9](#_Toc180675026)

[Pergunta 9 - What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if IPs are identified as Cobalt Strike C2 servers. 9](#_Toc180675027)

[pergunta 10 - What is the Host header for the first Cobalt Strike IP address from the previous question? 11](#_Toc180675028)

[pergunta 11 - What is the domain name for the first IP address of the Cobalt Strike server? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab). 11](#_Toc180675029)

[pergunta 12 - What is the domain name for the first IP address of the Cobalt Strike server? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab). 12](#_Toc180675030)

[pergunta 13 - What is the domain name of the post-infection traffic? 12](#_Toc180675031)

[pergunta 14 - What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic? 12](#_Toc180675032)

[pergunta 15 - What was the length for the first packet sent out to the C2 server? 13](#_Toc180675033)

[pergunta 16 - What was the Server header for the malicious domain from the previous question? 13](#_Toc180675034)

[pergunta 17 - The malware used an API to check for the IP address of the victim’s machine. What was the date and time when the DNS query for the IP check domain occurred? (answer format: yyyy-mm-dd hh:mm:ss UTC) 13](#_Toc180675035)

[pergunta 18 - What was the domain in the DNS query from the previous question? 14](#_Toc180675036)

[pergunta 19 - Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic? 14](#_Toc180675037)

[pergunta 20 - How many packets were observed for the SMTP traffic? 14](#_Toc180675038)

[Conclusão 14](#_Toc180675039)

Contextualização

Carnage é uma sala da plataforma TryHackme de nível de dificuldade intermediária focada em segurança defensiva. Essa sala aborda as etapas realizadas pelo departamento SOC de uma empresa por meio do uso da ferramenta Wireshark.

Desenvolvimento

Pergunta 1 - What was the date and time for the first HTTP connection to the malicious IP?

Primeiramente, abrimos a file *carnage.pcap* no Wireshark.

Aplicamos o filtro “http” na barra de filtros de exibição para visualizarmos apenas frames HTTP.

Interface gráfica do usuário, Aplicativo, Tabela

Descrição gerada automaticamente

Ordenando os pacotes por ordem cronológica, encontramos a primeira conexão http realizada.

Para verificar a data em que esta conexão foi realizada, precisamos converter o valor de timestamp para a formatação de data convencional. Podemos fazer isso acessando o item View da Toolbar e alterando o Time Display Format para Date and Time of day.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Fazendo isso, verificamos que a primeira conexão http ocorreu em 2021-09-24 16:44:38.

Interface gráfica do usuário, Aplicativo, Tabela

Descrição gerada automaticamente

Pergunta 2 - Wha tis the name of the zip file that was downloaded?

Verificando a coluna Info do frame encontrado anteriormente, descobrimos que se trata de uma requisição GET.

Interface gráfica do usuário, Aplicativo

Descrição gerada automaticamente

A foi baixada foi documents.zip.

Pergunta 3 - What was the domain hosting the malicious zip file?

Verificando os Detalhes do Frame, podemos obter mais informações sobre o host do zip malicioso. Na sessão Hypertext Transfer Protocol, encontramos o domínio contendo o zip malicioso: attirenepal.com.

Uma imagem contendo Texto

Descrição gerada automaticamente

Pergunta 4 - Without downloading the file, what is the name of the file in the zip file?

Podemos analisar o fluxo TCP do frame para encontrar o nome do arquivo enviado dentro do arquivo zip. Para isso, selecionamos o frame e utilizamos o comando Follow TCP Stream.

Interface gráfica do usuário, Aplicativo, Tabela, Excel

Descrição gerada automaticamente

No TCP Stream, encontramos o nome do arquivo enviado dentro do zip: chart-1530076591.xls.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente com confiança média

Pergunta 5 - What is the name of the webserver of the malicious IP from which the zip file was downloaded?

Também é possível encontrar o nome do webserver no TCP Stream do frame: LiteSpeed.

Texto

Descrição gerada automaticamente

Pergunta 6 - What is the version of the webserver from the previous question?

A versão do Webserver da mesma forma que o nome, no TCP stream.



Pergunta 7 - Malicious files were downloaded to the victim host from multiple domains. What were the three domains involved with this activity?

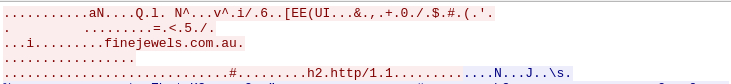
Na dica deixada para essa questão, descobrimos que o tipo e o horário em que os pacotes que precisamos encontrar foram enviados.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente

Após encontrar os IPs, basta seguir o TCP Stream e encontramos os domínios desejados.

O primeiro domínio encontrado foi finejewels.com.au.



O próximo domínio encontrado foi thietbiagt.com

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente com confiança média

Por fim, encontramos o domínio new.americold.com.

Tela de celular com texto preto sobre fundo branco

Descrição gerada automaticamente com confiança média

Pergunta 8 - Which certificate authority issued the SSL certificate to the first domain from the previous question?

Analisando novamente o TCP Stream do primeiro domínio, encontramos a autoridade que emitiu o certificado: Godaddy.



Pergunta 9 - What are the two IP addresses of the Cobalt Strike servers? Use VirusTotal (the Community tab) to confirm if IPs are identified as Cobalt Strike C2 servers.

Para facilitar a visualização dos frames, acessamos a sessão de Conversations do Wireshark por meio do item Statistics da Toolbar.

Interface gráfica do usuário, Texto, Tabela

Descrição gerada automaticamente

Em seguida, procuramos por IPs suspeitos e verificamos na plataforma VirusTotal se esses IPs se tratam de Cobalt Strike.

O primeiro IP encontrado foi 185.106.96.158. Acessando-o no VirusTotal, confirmamos que se trata de um servidor Cobalt Strike.

**Texto

Descrição gerada automaticamente**

O segundo IP encontrado foi 185.125.204.174, também se tratando de um servidor Cobalt Strike.

Texto

Descrição gerada automaticamente

pergunta 10 - What is the Host header for the first Cobalt Strike IP address from the previous question?

Seguindo o TCP Stream do primeiro IP encontrado, encontramos o seu host header.

Uma imagem contendo Texto

Descrição gerada automaticamente

pergunta 11 - What is the domain name for the first IP address of the Cobalt Strike server? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab).

O nome de domínio do servidor Cobalt Strike pode ser encontrado no comentário deixado no site VirusTotal.

Texto

Descrição gerada automaticamente

pergunta 12 - What is the domain name for the first IP address of the Cobalt Strike server? You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab).

Do mesmo modo, encontramos o nome de domínio do segundo servidor Cobalt Strike no seu respectivo comentário deixado no site VirusTotal.

Texto

Descrição gerada automaticamente

pergunta 13 - What is the domain name of the post-infection traffic?

Podemos filtrar apenas frames que possuem o método http post.



Seguindo o TCP Stream do primeiro frame encontrado, encontramos o nome de domínio.



pergunta 14 - What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?

Analisando a coluna Info do frame, temos os onze primeiros caracteres enviados pelo usuário: zLIisQRWZI9.



pergunta 15 - What was the length for the first packet sent out to the C2 server?

O tamanho do frame pode ser encontrado na coluna length.



pergunta 16 - What was the Server header for the malicious domain from the previous question?

Analisando novamente o TCP Stream do frame, encontramos o server header do domínio malicioso.

Uma imagem contendo Texto

Descrição gerada automaticamente

pergunta 17 - The malware used an API to check for the IP address of the victim’s machine. What was the date and time when the DNS query for the IP check domain occurred? (answer format: yyyy-mm-dd hh:mm:ss UTC)

Podemos filtrar apenas os frames que têm protocolo dns e que possuem uma api no nome.

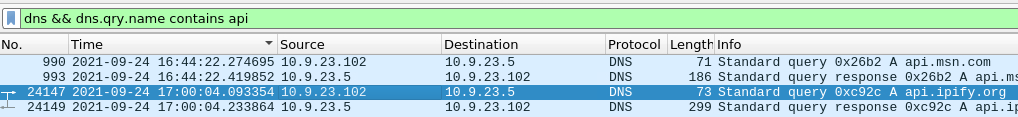
Interface gráfica do usuário, Aplicativo, Tabela, Excel

Descrição gerada automaticamente

Fazendo isso, encontramos o frame desejado e seu Time.

pergunta 18 - What was the domain in the DNS query from the previous question?

Encontramos o domínio na coluna Info do frame.



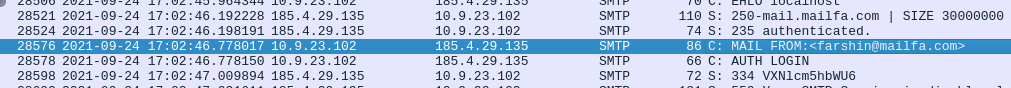
pergunta 19 - Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic?

Para encontrarmos spams maliciosos, filtramos os frames por protocolo SMTP, um protocolo utilizado para transmissão de e-mails.

Interface gráfica do usuário, Aplicativo, Tabela, Excel

Descrição gerada automaticamente

Explrorando os frames, encontramos o e-mail desejado.



pergunta 20 - How many packets were observed for the SMTP traffic?Parte superior do formulário

Para verificar o número de pacotes, basta olhar o mostrador no canto inferior direito do Wireshark.

****

Conclusão

A sala carnage é muito interessante para aprender a utilizar o Wireshark e o processo de análise de frames. Além disso, a sala aborda conceitos importantes sobre redes e protocolos que são essenciais para a área de cyber segurança.

**Referências**

<https://www.virustotal.com/gui/ip-address/>

<https://book.hacktricks.xyz/>