Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

carnage – TryHackMe

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | carnage – Enrico Santarelli |
| **N° Revisão** | 1 |
| **Data de publicação** | 30/08/2024 |
| **Link** | <https://tryhackme.com/r/room/c2carnage> |

|  |  |  |
| --- | --- | --- |
| **Redação** | Enrico | Membro |
| **Revisão** | Nome do revisor | Orientador |
| **Aprovação** | Nome do aprovador | Diretor |

|  |  |  |
| --- | --- | --- |
| **Histórico de revisões** | | |
| **N°** | **Entregas** | **Descrição** |
| **0** | 30/08/2024 | Produção |
| **1** | DD/MM/AAAA | Revisão |
| **2** | DD/MM/AAAA | Aprovação |

**Sumário**

[Contextualização 3](#_heading=h.gjdgxs)

[Desenvolvimento 3](#_heading=h.1fob9te)

[What was the date and time for the first HTTP connection to the malicious IP? 3](#_heading=h.3znysh7)

[What is the name of the zip file that was downloaded? 3](#_heading=h.2et92p0)

[What was the domain hosting the malicious zip file? 3](#_heading=h.tyjcwt)

[Without downloading the file, what is the name of the file in the zip file? 3](#_heading=h.3dy6vkm)

[What is the name of the webserver of the malicious IP from which the zip file was downloaded? 3](#_heading=h.tyjcwt)

[Malicious files were downloaded to the victim host from multiple domains. What were the threedomains involved with this activity? 3](#_heading=h.3dy6vkm)

[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. (answer format: enter the IP addresses in sequential order) 3](#_heading=h.tyjcwt)

[What is the Host header for the first Cobalt Strike IP address from the previous question? 3](#_heading=h.3dy6vkm)

[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). 3](#_heading=h.tyjcwt)

[What is the domain name of the second Cobalt Strike server IP?  You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab). 3](#_heading=h.3dy6vkm)

[What are the first eleven characters that the victim host sends out to the malicious domain involved in the post-infection traffic?  3](#_heading=h.tyjcwt)

[What was the length for the first packet sent out to the C2 server? 3](#_heading=h.3dy6vkm)

[What was the Server header for the malicious domain from the previous question? 3](#_heading=h.3dy6vkm)

[The malware used an API to check for the IP address of the victim’s machine. What was the date and time when theDNSquery for the IP check domain occurred? 3](#_heading=h.3dy6vkm)

[What was the domain in the DNS query from the previous question? 3](#_heading=h.3dy6vkm)

[Looks like there was some malicious spam (malspam) activity going on. What was the first MAIL FROM address observed in the traffic? 3](#_heading=h.3dy6vkm)

[How many packets were observed for the SMTPtraffic? 3](#_heading=h.3dy6vkm)

[Conclusão 3](#_heading=h.1t3h5sf)

[Referências 3](#_heading=h.4d34og8)

**Contextualização**

O foco dessa sala é praticar conhecimentos de investigação de pacotes no Wireshark e de potenciais atividades maliciosas neles. É importante para sala ter conhecimento prévio de comunicação entre dispositivos nas redes, principalmente detalhes de protocolos HTTP, HTTPs e SMTP.

**Desenvolvimento**

**What was the date and time for the first HTTP connection to the malicious IP?**

Para encontrar a primeira conexão HTTP com o IP malicioso é necessário filtrar os pacotes por handshakes de sincronização do cliente (tls.handshake.type eq 1). Ref: <https://medium.com/@parkerbenitez/wireshark-traffic-and-malware-analysis-2a5da9b5a610>

Interface gráfica do usuário, Aplicativo, Tabela, Excel

Descrição gerada automaticamente

R: 2021-09-24 16:44:38.

**What is the name of the zip file that was downloaded?**

Encontrado o IP malicioso, bastou filtrar a requisição HTTP pelo IP encontrado e checar o pacote com transferência de arquivo.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

R: documents.zip

**What was the domain hosting the malicious zip file?**

Para o domínio, foi necessário explorar o cabeçalho HTTP do pacote com o arquivo.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

R: attirenepal.com

**Without downloading the file, what is the name of the file in the zip file?**

Para o nome do arquivo na pasta teve-se que rastrear o pacote pelo pacote HTTP e verificar o seu conteúdo.

O nome do arquivo estava exposto no conteúdo da requisição meio à caracteres aleatórios.

Texto

Descrição gerada automaticamente

R: chart-1530076591.xls

**What is the name of the webserver of the malicious IP from which the zip file was downloaded?**

O nome do servidor estava presente no cabeçalho do pacote apresentado na questão anterior, através da propriedade “server”.

R: LiteSpeed

**What is the version of the webserver from the previous question?**

A versão do servidor estava presente no cabeçalho do pacote apresentado na questão anterior, através da propriedade “x-powered-by”.

R: PHP/7.2.34

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

A dica do TryHackMe indicava que seria necessário aplicar alguns filtros específicos para essa questão.

Interface gráfica do usuário, Texto

Descrição gerada automaticamente com confiança média

Aplicando esses filtros: frame.time >= "2021-09-24 16:45:11" and frame.time < "2021-09-24 16:45:30" and ssl.

O ssl do comando representa a camada de criptografia da requisição HTTPS, portanto filtra os pacotes como HTTPS.

Tabela

Descrição gerada automaticamente

Para encontrar o nome dos domínios foi necessário procurar pelos pacotes de handshake de sincronização (Client Hello):

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

R: finejewels.com.au, thietbiagt.com, new.americold.com

**Which certificate authority issued the SSL certificate to the first domain from the previous question?**

Para isso, tivemos que procurar pelo pacote HTTPS do IP em questão que tivesse como info “Certificate”. O domínio do certificado SSL está presente na descrição do protocolo de handshake.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

R: GoDaddy

**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. (answer format: enter the IP addresses in sequential order)**

Para essa questão foi necessário entrar na aba “Conversations” em “Statistics” e listar todos os IPs envolvidos nas conversas. A partir deles procurar na comunidade do VirusTotal os pertencentes à Cobal Strike.

Interface gráfica do usuário, Tabela

Descrição gerada automaticamente com confiança média

<https://www.virustotal.com/gui/ip-address/185.106.96.158/community>

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

<https://www.virustotal.com/gui/ip-address/185.125.204.174/community>

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

R: 185.106.96.158, 185.125.204.174

**What is the Host header for the first Cobalt Strike IP address from the previous question?**

Para responder isso filtramos os pacotes pelo IP do atacante e encontramos o host no cabeçalho do HTTP.

Uma imagem contendo Tabela

Descrição gerada automaticamente

R: ocsp.verisign.com

**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).**

Para essa questão utilizamos a listagem de domínios DNS da virustotal para o domínio.

<https://www.virustotal.com/gui/ip-address/185.106.96.158/relations>

Tela de computador

Descrição gerada automaticamente

R: survmeter.live

**What is the domain name of the second Cobalt Strike server IP?  You may use VirusTotal to confirm if it's the Cobalt Strike server (check the Community tab).**

Para essa questão utilizamos a listagem de domínios DNS da virustotal para o domínio.

<https://www.virustotal.com/gui/ip-address/185.125.204.174/relations>

Tela de celular com fundo preto

Descrição gerada automaticamente

R: securitybusinpuff.com

**What is the domain name of the post-infection traffic?**

Nesse caso, como procuramos por requisições post, filtramos os pacotes por esse método. Logo nos deparamos com uma sequência de requisições “estranhas” que continham em seu cabeçalho o host de origem.

Texto

Descrição gerada automaticamente

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

R: maldivehost.net

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

**Parte superior do formulário**

Para respondê-la apenas foi necessário pegar os primeiros 11 caracteres da sequência de caracteres “estranhos” dos pacotes.

R: zLIisQRWZI9

**What was the length for the first packet sent out to the C2 server?**

O tamanho do pacote fica exposto em “Frame” ao clicar no pacote.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

R: 281

**What was the Server header for the malicious domain from the previous question?**

O servidor está exposto no cabeçalho de “Server” do pacote HTTP na questão anterior.

R: Apache/2.4.49 (cPanel) OpenSSL/1.1.1l mod\_bwlimited/1.4

**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)**

Nesse caso, foi necessário filtrar os pacotes por DNS e também procurar por palavras “api” através da palavra “contains”.

Tabela

Descrição gerada automaticamente

R: 2021-09-24 17:00:04

**What was the domain in the DNS query from the previous question?**

O domínio do pacote analisado na questão anterior estava exposto na própria info do pacote.

R: api.ipify.org

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

Conexões via e-mail podem passar por três protocolos: POP, IMAP, SMTP. O e-mail procurado na questão foi encontrado ao filtrar pelo protocolo SMTP e estava exibido na info do pacote.

Tabela

Descrição gerada automaticamente com confiança média

R: [farshin@mailfa.com](mailto:farshin@mailfa.com)

**How many packets were observed for the SMTP traffic?**

O Wireshark conta os pacotes de acordo com os protocolos e disponibiliza esses valores na aba “Statistics” e “Protocol Hierarchy”.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Tabela

Descrição gerada automaticamente

R: 1439

**Conclusão**

Esse CTF é muito interessante para aqueles que querem explorar conteúdos diferentes de segurança e fugir dos padrões de CTF. Eu indicaria principalmente para quem quer aprender mais sobre o uso de Wireshark.

Reforço a possível necessidade de conhecimentos prévios de protocolos de rede e comunicação entre dispositivos.

**Referências**

* https://www.virustotal.com/gui/ip-address/
* <https://medium.com/@parkerbenitez/wireshark-traffic-and-malware-analysis-2a5da9b5a610>