Uma imagem contendo Logotipo

Descrição gerada automaticamente

Relatório de CTF

Warzone 1 – Tryhakme

|  |  |
| --- | --- |
| **Informações do documento** | |
| **Referência** | Warzone 1 – Sérgio Guidi Trovo |
| **N° Revisão** | 1 |
| **Data de publicação** | 03/11/2024 |
| **Link** | <https://tryhackme.com/r/room/warzoneone> |

|  |  |  |
| --- | --- | --- |
| **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

[Sumário 2](#_Toc181541368)

[Contextualização 3](#_Toc181541369)

[Desenvolvimento 3](#_Toc181541370)

[Pergunta 1 - What was the alert signature for Malware Command and Control Activity Detected? 3](#_Toc181541371)

[Pergunta 2 - What is the source IP address? Enter your answer in a defanged format. 4](#_Toc181541372)

[Pergunta 3 - What IP address was the destination IP in the alert? Enter your answer in a defanged format. 5](#_Toc181541373)

[Pergunta 4 - Inspect the IP address in VirusTotal. Under Relations > Passive DNS Replication, which domain has the most detections? Enter your answer in defanged format. 5](#_Toc181541374)

[Pergunta 5 - Still in VirusTotal, under Community, what threat group is attributed to this IP address? 6](#_Toc181541375)

[Pergunta 6 - What is the malware family? 6](#_Toc181541376)

[Pergunta 7 - Do a search in VirusTotal for the domain from question 4. What was the majority file type listed under Communicating Files? 7](#_Toc181541377)

[Pergunta 8 - Inspect the web traffic for the flagged IP address; what is the user-agent in the traffic? 7](#_Toc181541378)

[Pergunta 9 - Retrace the attack; there were multiple IP addresses associated with this attack. What were two other IP addresses? Enter the IP addressed defanged and in numerical order. (format: IPADDR,IPADDR) 8](#_Toc181541379)

[Pergunta 10 - What were the file names of the downloaded files? Enter the answer in the order to the IP addresses from the previous question. (format: file.xyz,file.xyz) 10](#_Toc181541380)

[Pergunta 11 - Inspect the traffic for the first downloaded file from the previous question. Two files will be saved to the same directory. What is the full file path of the directory and the name of the two files? (format: C:\path\file.xyz,C:\path\file.xyz) 11](#_Toc181541381)

[Pergunta 12 - Now do the same and inspect the traffic from the second downloaded file. Two files will be saved to the same directory. What is the full file path of the directory and the name of the two files? (format: C:\path\file.xyz,C:\path\file.xyz) 12](#_Toc181541382)

[Conclusão 13](#_Toc181541383)

[Referências 13](#_Toc181541384)

Contextualização

Warzone 1 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 alert signature for Malware Command and Control Activity Detected?

Podemos utilizar o software Brim para analisar o tráfego de rede da file Zone1.pcap. Parte superior do formulário

Primeiro filtramos apenas files que contenham a categoria de alerta desejado.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Na coluna de alert signature, encontramos a resposta para a primeira pergunta.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Pergunta 2 - What is the source IP address? Enter your answer in a defanged format.

Analisamos a coluna de src\_ip do frame encontrado.



Podemos utilizar o software Cyberchef para transformar o endereço IP para o formato defanged. Inserimos o endereço IP na sessão de input.

Interface gráfica do usuário

Descrição gerada automaticamente

Adicionamos a Recipe *Defang IP Addresses.*

Retângulo

Descrição gerada automaticamente

Na sessão de output, obtemos a resposta.

Interface gráfica do usuário

Descrição gerada automaticamente com confiança baixa

Pergunta 3 - What IP address was the destination IP in the alert? Enter your answer in a defanged format. Parte superior do formulário

Realizamos os mesmos passos da pergunta anterior, dessa vez utilizando o endereço IP da coluna dest\_ip.

Interface gráfica do usuário, Texto, Aplicativo, chat ou mensagem de texto

Descrição gerada automaticamente

Obtemos o resultado novamente por meio da ferramenta Cyberchef.

Interface gráfica do usuário, Texto, Aplicativo, Word

Descrição gerada automaticamente

Pergunta 4 - Inspect the IP address in VirusTotal. Under Relations > Passive DNS Replication, which domain has the most detections? Enter your answer in defanged format.

Acessando o site VirusTotal e pesquisando pelo endereço IP, encontramos o domínio com mais detecções.

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

Pergunta 5 - Still in VirusTotal, under Community, what threat group is attributed to this IP address?

Acessando a aba de Community, encontramos diversos usuários citando o threat group do endereço de IP: TA505.

Tela de computador com fundo preto

Descrição gerada automaticamente

Pergunta 6 - What is the malware family?

A malware family também pode ser encontrado em diversos comentários deixados no site VirusTotal: MirrorBlast.

Pergunta 7 - Do a search in VirusTotal for the domain from question 4. What was the majority file type listed under Communicating Files?



Encontramos que o tipo da file é Windows Installer.

Pergunta 8 - Inspect the web traffic for the flagged IP address; what is the user-agent in the traffic?

Para encontrar o user-agent do endereço IP, abrimos a file Zone1.pcap no software Wireshark. Filtramos apenas frames com o endereço IP desejado.

Tabela

Descrição gerada automaticamente

Seguimos o TCP Stream do segundo frame mostrado que tem como source o endereço IP desejado.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

No TCP Stream, encontramos o user-agent.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Pergunta 9 - Retrace the attack; there were multiple IP addresses associated with this attack. What were two other IP addresses? Enter the IP addressed defanged and in numerical order. (format: IPADDR,IPADDR)

Podemos utilizar a sessão de conversations do Wireshark para verificar os endereços de IP com os quais a máquina analisada se comunicou. Para isso, acessamos o item Statistics da Toolbar e clicamos em conversations.

Interface gráfica do usuário, Texto, Aplicativo

Descrição gerada automaticamente

Tabela

Descrição gerada automaticamente

Utilizando o site VirusTotal, podemos encontrar os endereços IP associados com o ataque.

Tela de celular com aplicativo aberto

Descrição gerada automaticamente

Tela de celular com aplicativo aberto

Descrição gerada automaticamente

Encontramos esses dois endereços de IP com a mesma malware Family que a do ataque.

Pergunta 10 - What were the file names of the downloaded files? Enter the answer in the order to the IP addresses from the previous question. (format: file.xyz,file.xyz)

Aplicando o primeiro endereço encontrado na pergunta anterior como filtro no Wireshark, temos listados os frames trocados entre o servidor e esse endereço.

Interface gráfica do usuário, Aplicativo, Tabela, Excel

Descrição gerada automaticamente

Seguindo o TCP Stream do primeiro frame, encontramos o nome da primeira file baixada.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Aplicando os mesmos passos para o segundo endereço de IP, encontramos a segunda file baixada.

Interface gráfica do usuário, Texto, Aplicativo, Email

Descrição gerada automaticamente

Pergunta 11 - Inspect the traffic for the first downloaded file from the previous question. Two files will be saved to the same directory. What is the full file path of the directory and the name of the two files? (format: C:\path\file.xyz,C:\path\file.xyz)

Podemos analisar novamente o TCP Sream do primeiro frame analisado na questão anterior. Procuramos por “C:\” na barra Find e encontramos a path para o diretório em que os arquivos foram baixados e os arquivos que foram baixados.

Texto

Descrição gerada automaticamente

Pergunta 12 - Now do the same and inspect the traffic from the second downloaded file. Two files will be saved to the same directory. What is the full file path of the directory and the name of the two files? (format: C:\path\file.xyz,C:\path\file.xyz)

Aplicando os mesmos passos que para a questão anterior, encontramos a path para o diretório e as files que foram salvas.Parte superior do formulário

Texto

Descrição gerada automaticamente

Conclusão

A sala Warzone 1 é uma ótima sala para aprender a utilizar ferramentas importantes do processo de segurança defensiva. Essa sala foca na análise de logs.

Referências

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

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

<https://gchq.github.io/CyberChef/>