Laboratório - Investigando um Ataque a um Host Windows .

# Objetivos

Neste laboratório, você irá:

Parte 1: Investigar o Ataque com Sguil

Parte 2: Usar o Kibana para investigar alertas

Este laboratório é baseado em um exercício do site malware-traffic-analysis.net, que é um excelente recurso para aprender a analisar ataques de rede e host. Agradecemos a brad@malware-traffic-analysis.net para permissão para usar materiais de seu site.

# Histórico/Cenário

Em março de 2019, as ferramentas de monitoramento de segurança de rede alertaram que um computador Windows na rede estava infectado com malware. Nesta tarefa, você deve investigar os alertas e responder às seguintes perguntas:

* Qual foi o tempo específico do ataque em 2019-03-19?
* Qual computador host do Windows foi infectado? Quem era o usuário?
* Com o que o computador estava infectado?

# Recursos necessários

* Máquina virtual Security Onion
* Acesso à Internet

# Instruções

## Investigar o Ataque com Sguil

Na Parte 1, você usará o Sguil para verificar os alertas IDS e coletar mais informações sobre a série de eventos relacionados a um ataque em 3-19-2019.

**Observação**: Os IDs de alerta usados neste laboratório são, por exemplo, apenas. Os IDs de alerta em sua VM podem ser diferentes.

### Abra o Sguil e localize os alertas no 3-19-2019.

* + - 1. Faça login no Security Onion VM com o nome de usuário do **analyst** e a senha do **cyberops**.
      2. Inicie o Sguil a partir da área de trabalho. Faça login com **analyst** de nome de usuário e **cyberops**de senha. Clique em **Select All** e **Start Sguil** para exibir todos os alertas gerados pelos sensores de rede.
      3. Localize o grupo de alertas a partir de 19 de março de 2019.

#### Pergunta:

De acordo com Sguil, quais são os carimbos de data/hora para o primeiro e último dos alertas que ocorreram em 3-19-2019? O que é interessante sobre os carimbos de data/hora de todos os alertas em 3-19-2019?

Digite suas respostas aqui.

### Revise os alertas detalhadamente.

* + - 1. No Sguil, clique no primeiro dos alertas em 3-19-2019 (Alert ID 5.439). Certifique-se de marcar as caixas de seleção **Show Packet Data** e **Show Rule** para examinar as informações do cabeçalho do pacote e a regra de assinatura do IDS relacionada ao alerta. Direto no **ID de alerta** e mude para Wireshark. Com base nas informações derivadas deste alerta inicial, responda às seguintes perguntas:

#### Perguntas:

Qual era o endereço IP de origem e o número da porta e o endereço IP de destino e o número da porta?

Digite suas respostas aqui.

Que tipo de protocolo e solicitação ou resposta estava envolvido?

Digite suas respostas aqui.

O que é o alerta e a mensagem IDS?

Digite suas respostas aqui.

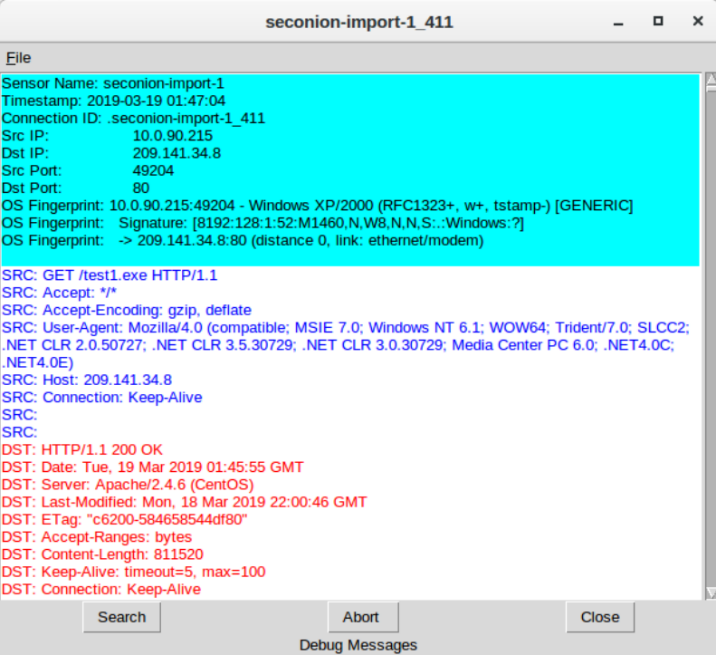
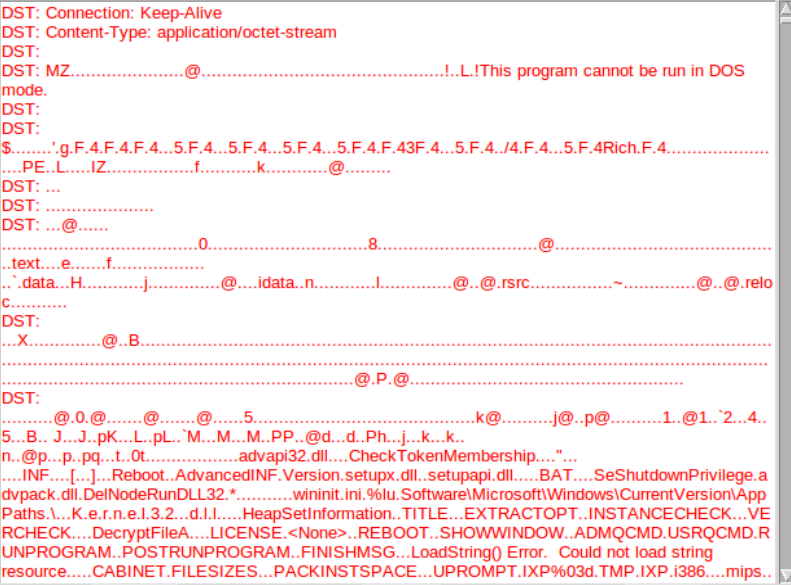
Você acha que esse alerta foi resultado de um erro de configuração do IDS ou de uma comunicação suspeita legítima?

Digite suas respostas aqui.

Qual é o nome de host, nome de domínio e endereço IP do host de origem na atualização DNS?

Digite suas respostas aqui.

* + - 1. Em Sguil, selecione o segundo dos alertas em 3-19-2019. Clique com o botão direito do mouse no Alert ID 5.440 e selecione **Transcript**.

A partir da transcrição, responda às seguintes perguntas:

#### Perguntas:

Qual é o endereço IP de origem e destino e os números de porta?

Digite suas respostas aqui.

Olhando para o pedido (azul) para que era o pedido?

Digite suas respostas aqui.

Olhando para a resposta (vermelho), muitos arquivos revelarão sua assinatura de arquivo nos poucos caracteres iniciais do arquivo quando visualizados como texto. As assinaturas de arquivo ajudam a identificar o tipo de arquivo que é representado. Use um navegador da Web para procurar uma lista de assinaturas de arquivos comuns.

#### Pergunta:

Quais são os poucos caracteres iniciais do arquivo. Pesquisar esta assinatura de arquivo para descobrir que tipo de arquivo foi baixado nos dados?

Digite suas respostas aqui.

* + - 1. Feche a transcrição. Use o Wireshark para exportar o arquivo executável para análise de malware (**File** > **Export objects** > **HTTP...**). Salve o arquivo na pasta pessoal do analista.
      2. Abra um terminal na VM Security Onion e crie um hash SHA256 a partir do arquivo exportado. Use o seguinte comando:

analyst @SecOnion: ~$ **sha256sum test1.exe**

**2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85** test1.exe

* + - 1. Copie o hash do arquivo e envie-o para o Cisco Talos file reputation em <https://talosintelligence.com/talos_file_reputation>.

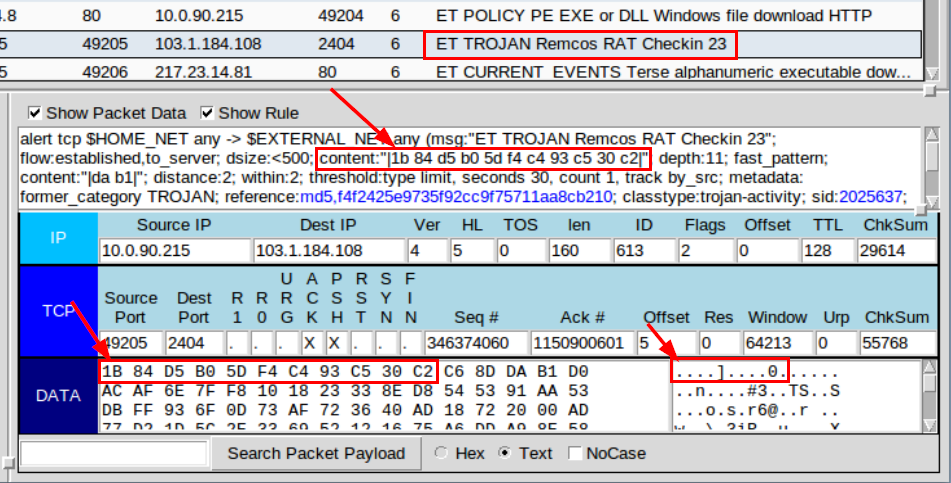


#### Pergunta:

O Talos reconheceu o hash do arquivo e o identificou como malware? Em caso afirmativo, que tipo de malware?

Digite suas respostas aqui.

* + - 1. No Sguil, selecione o **Alert ID 5.480** e o **Event Message** Remcos RAT Checkin 23. Observe que a assinatura IDS detectou o RAT Remcos com base nos códigos hexadecimais binários no início da comunicação.



* + - 1. Clique com o botão direito do mouse no ID de alerta e selecione **Transcript**. Percorra a transcrição e responda às seguintes perguntas:

#### Perguntas:

Qual é a porta de destino da comunicação? É um porta conhecida?

Digite suas respostas aqui.

A comunicação é legível ou criptografada?

Digite suas respostas aqui.

Faça alguma pesquisa online sobre Remcos RAT Checkin 23. O que significa Remcos?

Digite suas respostas aqui.

Que tipo de comunicação acha que estava sendo transmitida?

Digite suas respostas aqui.

Que tipo de criptografia e ofuscação foi usado para ignorar a detecção?

Digite suas respostas aqui.

* + - 1. Usando o Sguil e os alertas restantes do 3-19-2019, localize o segundo arquivo executável que foi baixado e verifique se ele é um malware conhecido.

#### Perguntas:

Quais IDs de alerta alertam para um segundo arquivo executável que está sendo baixado?

Digite suas respostas aqui.

De qual endereço IP do servidor e número da porta o arquivo foi baixado?

Digite suas respostas aqui.

Qual é o nome do arquivo que foi baixado?

Digite suas respostas aqui.

Crie um hash SHA256 do arquivo e envie o hash on-line no Cisco Talos File Reputation Center para ver se ele corresponde a malware conhecido. O arquivo executável é conhecido como malware e, em caso afirmativo, que tipo? O que é o AMP DETECTIN

Digite suas respostas aqui.

* + - 1. Examine os três alertas restantes de 3-19-2019 observando as informações de cabeçalho em Mostrar dados de pacote, a assinatura IDS em Mostrar regra e as transcrições de ID de alerta.

#### Pergunta:

Como todos os três alertas estão relacionados?

Digite suas respostas aqui.

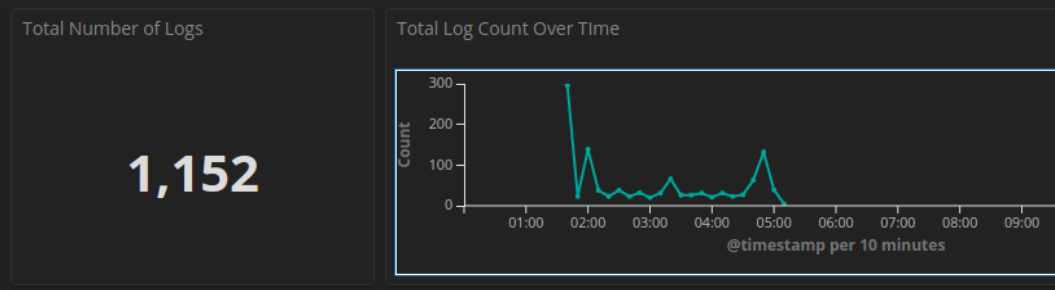
* + - 1. Mesmo que você tenha examinado todos os alertas no Sguil relacionados a um ataque em um host Windows em 3-19-2019, pode haver informações adicionais relacionadas disponíveis no Kibana. Feche o Sguil e inicie o Kibana a partir da área de trabalho.

## Usar o Kibana para investigar alertas

Na Parte 2, use Kibana para investigar mais detalhadamente o ataque em 3-19-2019.

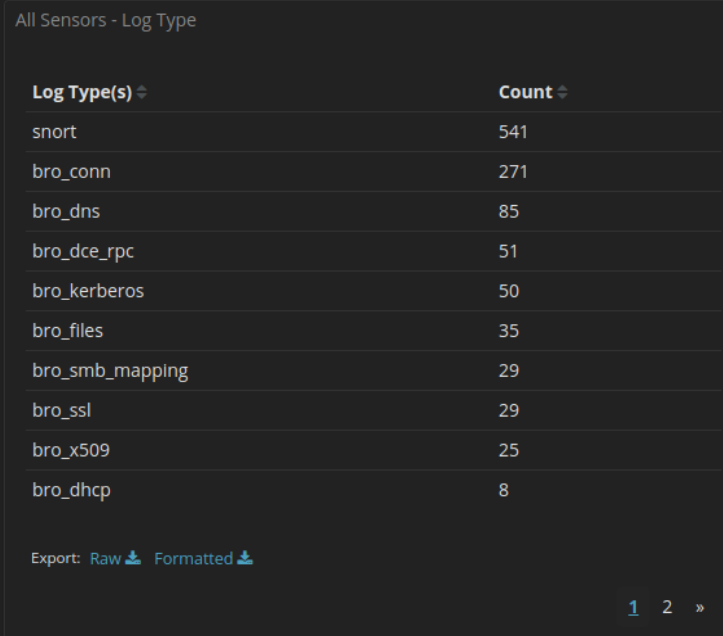
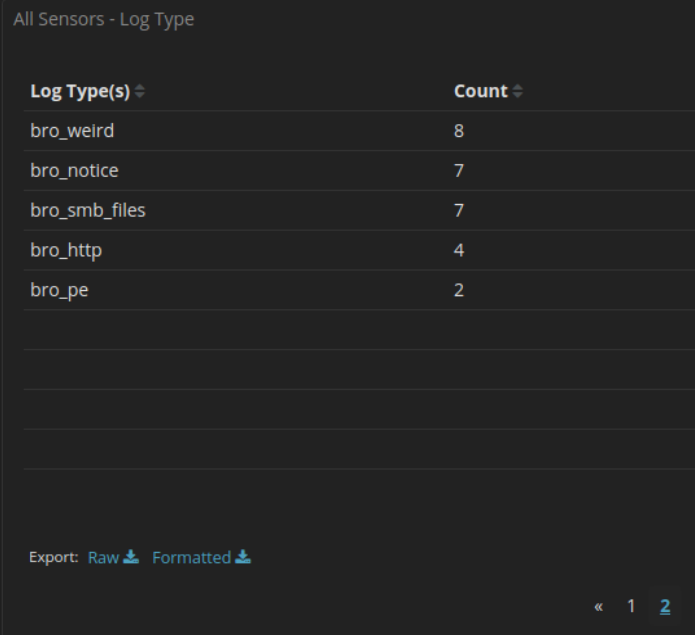
### Abra Kibana e reduza o período de tempo.

* + - 1. Faça login no Kibana com o nome de usuário do **analyst** e a senha do **cyberops**.
      2. Abra o Kibana ( **analyst** de nome de usuário e **cyberops**de senha), clique em **Last 24 Hours** e na guia Intervalo de tempo **Absolute** para alterar o intervalo de tempo para 1 de março de 2019 para 31 de março de 2019.
      3. A linha do **Total Log Count Over Time** do tempo mostrará um evento em 19 de março. Clique nesse evento para restringir o foco ao intervalo de tempo específico do ataque.

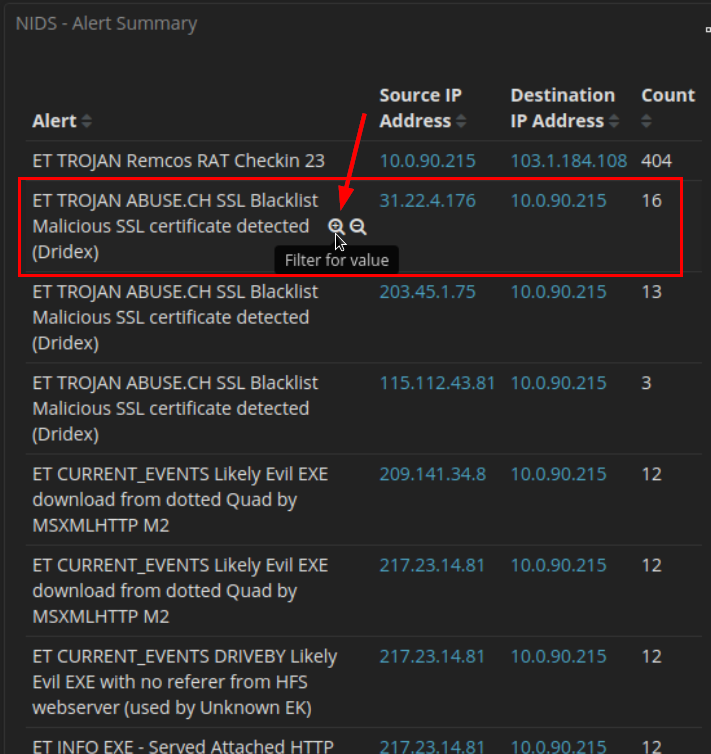


### Revise os alertas no período de tempo reduzido.

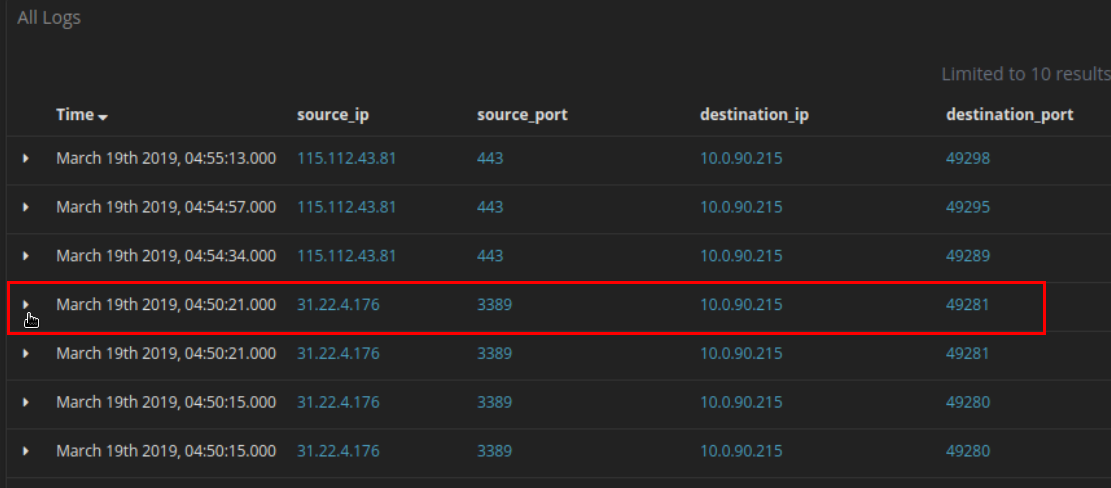
* + - 1. No painel Kibana, role para baixo até a visualização **Todos os Sensores - Tipo de Log**. Revise ambas as páginas e observe a variedade de tipos de log relacionados a esse ataque.

* + - 1. Role para baixo e observe que o Resumo de Alerta NIDS no Kibana tem muitos dos mesmos alertas IDS listados no Sguil. Clique na lupa para filtrar o segundo alerta ET TROJAN ABUSE.CH SSL Lista Negra SSL Certificado SSL Malicioso detectado (Dridex) do Endereço IP de Origem 31.22.4.176.



* + - 1. Role para baixo até All logs e clique na seta para expandir o primeiro log na lista com o endereço IP de origem 31.22.4.176.



#### Perguntas:

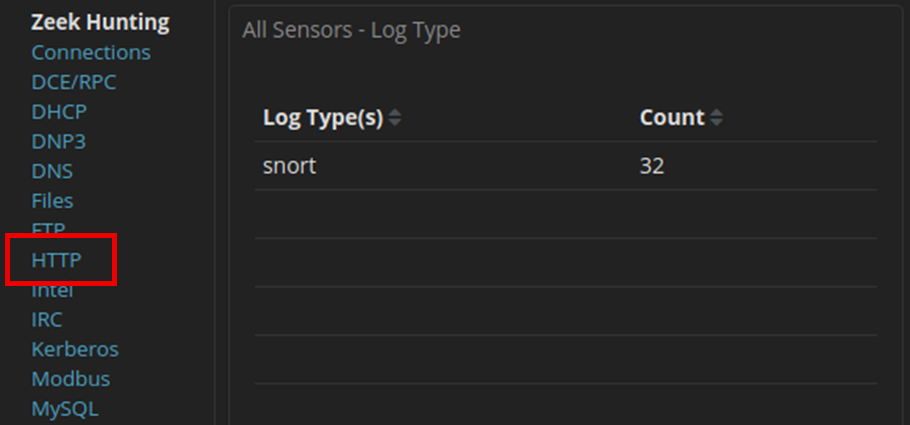
Qual é a localização geográfica do país e da cidade para este alerta?

Digite suas respostas aqui.

Qual é o país geográfico e a cidade para o alerta da 115.112.43.81?

Digite suas respostas aqui.

* + - 1. Role de volta para a parte superior da página e clique no link under Navigation.
      2. Anteriormente, observamos tipos de log como bro\_http listados no painel Início. Você pode filtrar para os vários tipos de log, mas os painéis internos provavelmente terão mais informações. Role de volta para o topo da página e clique em **HTTP** no link do painel em Zeek Hunting in Navigation.



* + - 1. Percorra o painel HTTP tomando conhecimento das informações apresentadas e responda às seguintes perguntas:

#### Perguntas:

O que é a contagem de logs no painel HTTP? De que países?

Digite suas respostas aqui.

Quais são os URIs para os arquivos que foram baixados?

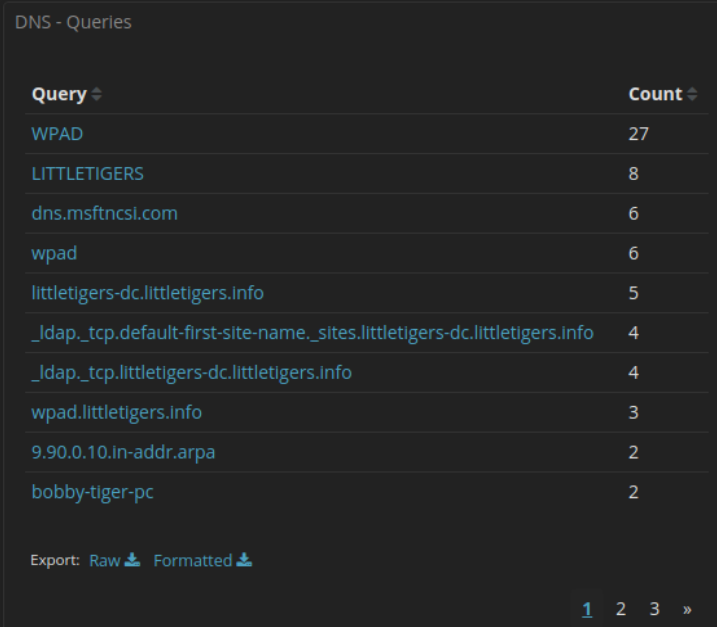
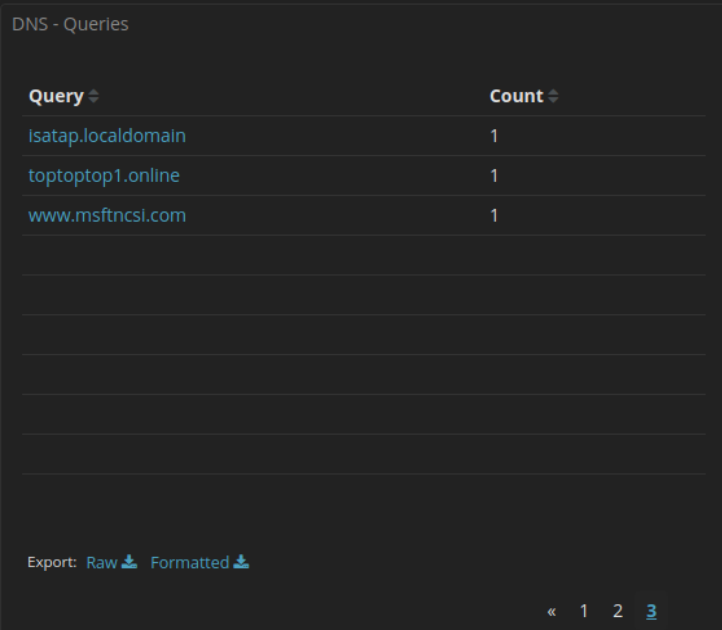
* + - 1. Corresponda o **HTTP - URIs** ao **HTTP - Sites** no painel.

#### Pergunta:

Quais são os arquivos Cspca.crl e ncsi.txt relacionados? Use um navegador da Web e um mecanismo de pesquisa para obter informações adicionais.

Digite suas respostas aqui.

* + - 1. Role de volta para o topo da página web e, em Navegação - Zeek Hunting, clique em **DNS**. Role até a visualização de consultas DNS. Observe a página 1 e a página 3 das consultas DNS.

Algum dos domínios parece potencialmente inseguro? Tente enviar o URL toptoptop1.online para virustotal.com. Qual é o resultado?

Digite suas respostas aqui.

* + - 1. Para mais investigação e curiosidade, tente examinar os seguintes painéis de caça Zeek:

DCE/RPC - para obter informações sobre os procedimentos remotos de rede do Windows e recursos envolvidos

Kerberos — para obter informações sobre os nomes de host e nomes de domínio que foram usados

PE — para obter informações sobre os executáveis portáteis

SSL e x.509 — para obter informações sobre os nomes dos certificados de segurança e os países que foram usados

SMB — para mais informações sobre as ações SMB na rede de littletigers

Estranho — para anomalias de protocolo e serviço e comunicações mal formadas

Fim do documento