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

Parte 1: 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.

Etapa 1: Abra o Sguil e localize os alertas no 3-19-2019.

a. Faça login no Security Onion VM com o nome de usuário do **analyst** e a senha do **cyberops**.

b. 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.

c. Localize o grupo de alertas a partir de 19 de março de 2019.

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?

Etapa 2: Revise os alertas detalhadamente.

a. 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:

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

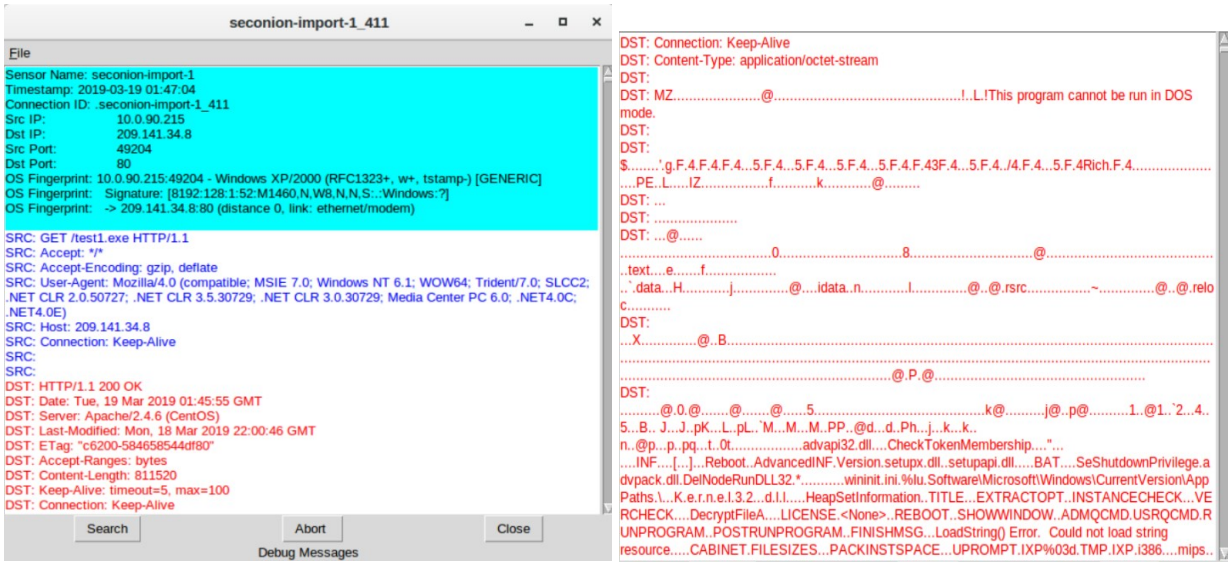
Que tipo de protocolo e solicitação ou resposta estava envolvido?

O que é o alerta e a mensagem IDS?

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

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

b. 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:

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

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

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.

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

c. 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.

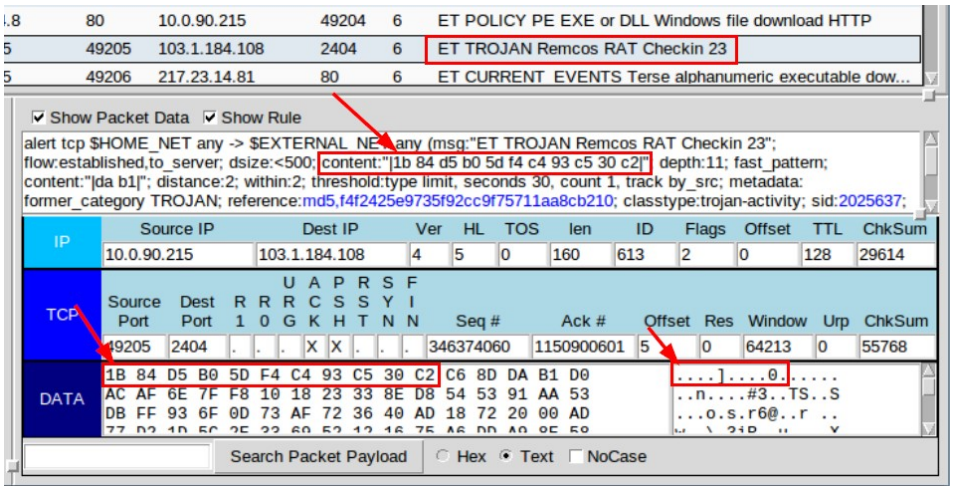
d. Abra um terminal na VM Security Onion e crie um hash SHA256 a partir do arquivo exportado. Use o seguinte comando:

```
analyst @SecOnion: ~$ sha256sum test1.exe
2a9b0ed40f1f0bc0c13ff35d304689e9cadd633781cbcad1c2d2b92ced3f1c85 test1.exe
```

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

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

f. 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.



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

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

A comunicação é legível ou criptografada?

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

Que tipo de comunicação acha que estava sendo transmitida?

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

h. 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.

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

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

Qual é o nome do arquivo que foi baixado?

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

i. 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.

Como todos os três alertas estão relacionados?

j. 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.

Parte 2: Usar o Kibana para investigar alertas

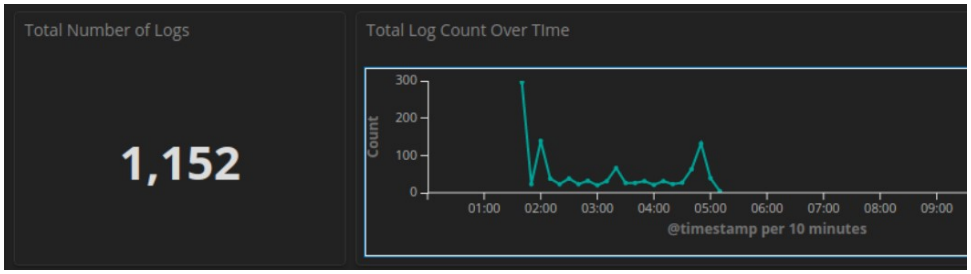
Na Parte 2, use Kibana para investigar mais detalhadamente o ataque em 3-19-2019.

Etapa 1: Abra Kibana e reduza o período de tempo.

a. Faça login no Kibana com o nome de usuário do **analyst** e a senha do **cyberops**.

b. 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.

c. 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.



Etapa 2: Revise os alertas no período de tempo reduzido.

a. 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.

All Sensors - Log Type

Log Type(s)	Count
snort	541
bro_conn	271
bro_dns	85
bro_dce_rpc	51
bro_kerberos	50
bro_files	35
bro_smb_mapping	29
bro_ssl	29
bro_x509	25
bro_dhcp	8

Export: Raw Formatted

1 2 »

All Sensors - Log Type

Log Type(s)	Count
bro_weird	8
bro_notice	7
bro_smb_files	7
bro_http	4
bro_pe	2

Export: Raw Formatted

« 1 2

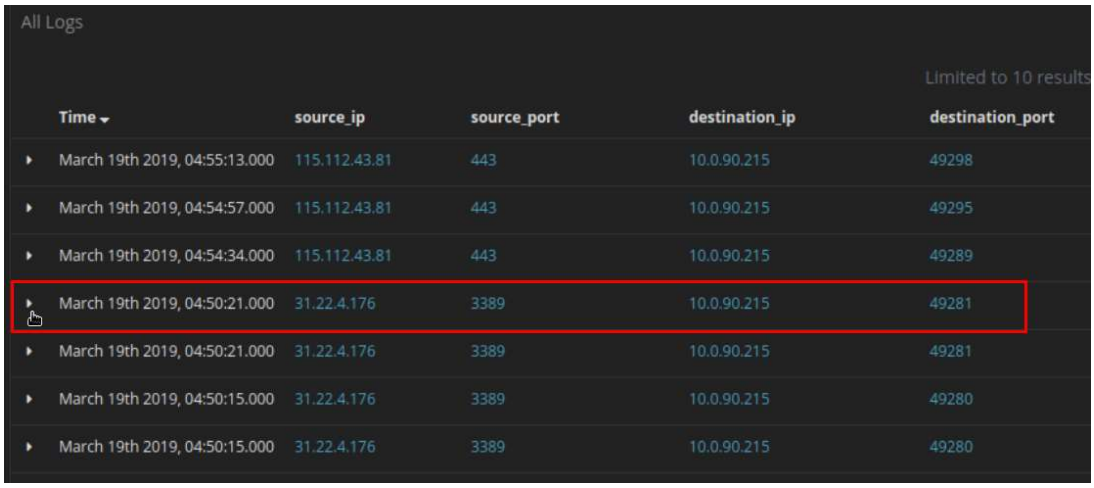
b. Role para baixo e observe que o Resumo de Alerta NIDS no Kibana tem muitos dos mesmos alertas IDS listados no Sguil. Clique na lupa para filtrar o segundo alerta ET TROJAN ABUSE.CH SSL Lista Negra SSL Certificado SSL Malicioso detectado (Dridex) do Endereço IP de Origem 31.22.4.176.

NIDS - Alert Summary

Alert	Source IP Address	Destination IP Address	Count
ET TROJAN Remcos RAT Checkin 23	10.0.90.215	103.1.184.108	404
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	31.22.4.176	10.0.90.215	16
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	203.45.1.75	10.0.90.215	13
ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	115.112.43.81	10.0.90.215	3
ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2	209.141.34.8	10.0.90.215	12
ET CURRENT_EVENTS Likely Evil EXE download from dotted Quad by MSXMLHTTP M2	217.23.14.81	10.0.90.215	12
ET CURRENT_EVENTS DRIVEBY Likely Evil EXE with no referer from HFS webserver (used by Unknown EK)	217.23.14.81	10.0.90.215	12
ET INFO EXE - Served Attached HTTP	217.23.14.81	10.0.90.215	12

Filter for value

c. 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.

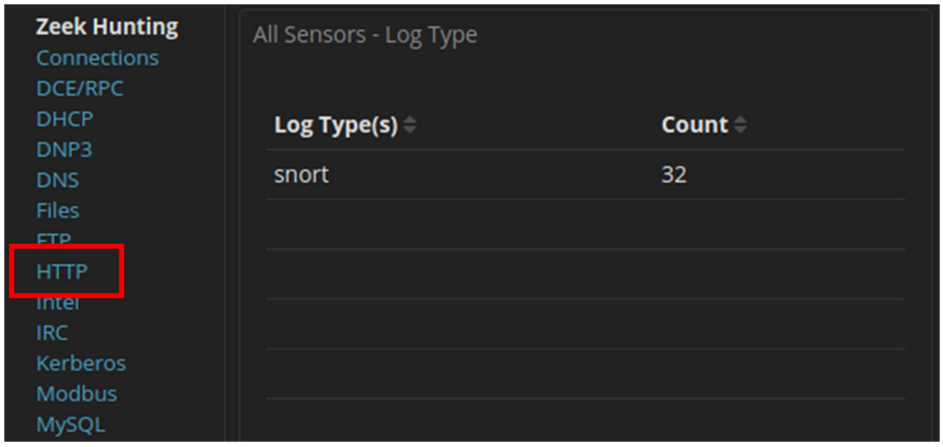


Qual é a localização geográfica do país e da cidade para este alerta?

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

d. Role de volta para a parte superior da página e clique no link under Navigation.

e. 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.



f. Percorra o painel HTTP tomando conhecimento das informações apresentadas e responda às seguintes perguntas:

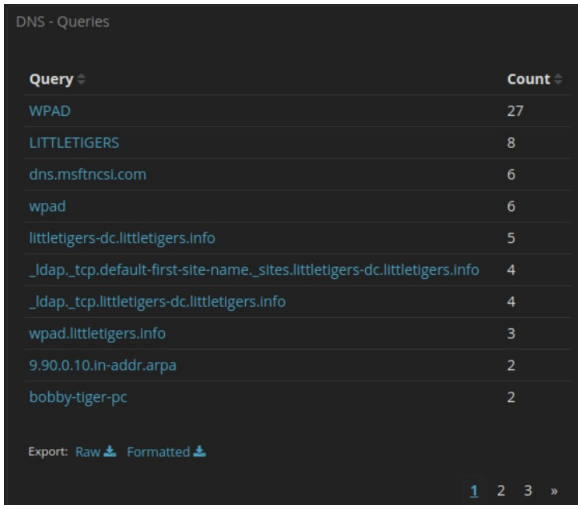
O que é a contagem de logs no painel HTTP? De que países?

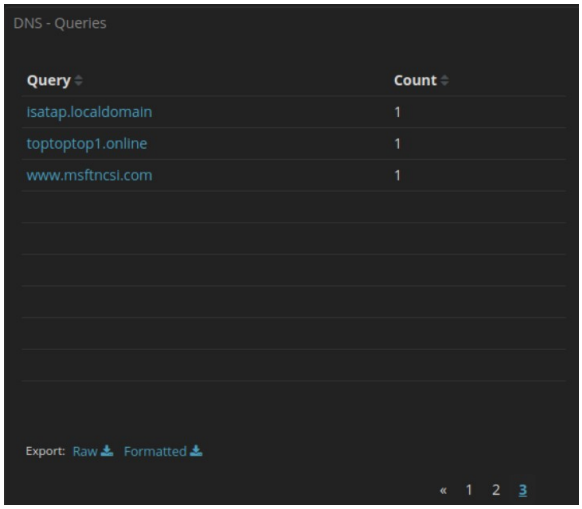
Quais são os URIs para os arquivos que foram baixados?

g. Corresponda o **HTTP - URIs** ao **HTTP - Sites** no painel.

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

h. 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?

i. 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