TryHackMe: Itsy Bitsy

Scenario - Investigate a potential C2 communication alert

Durante um monitoramento SOC, o analista John observou um alerta em uma solução IDS indicando uma comunicação C2 em potencial pelo usuário Browne do departamento de RH. Um arquivo suspeito foi acessado, contendo um padrão malicioso THM:{_____} . Logs de comunicação HTTP de uma semana foram pegos para investigação. Devido a recursos limitados, somente os logs de comunicação puderam ser pegos e estão ingeridos no index connection_logs no Kibana.

Nosso trabalho neste desafio será examinar os logs de conexão da rede deste usuário, achar o link e o conteúdo do arquivo, e responder as perguntas.

Abrindo a sala, temos um aviso de que não há dados na data atual, pois a configuração está de 15 minutos atrás até a atualidade. Colocando a data inicial em 1 de Janeiro de 2022 e a data final na data atual (18 de Maio de 2024), conseguiremos achar graficamente onde está a semana quando os dados foram coletados.

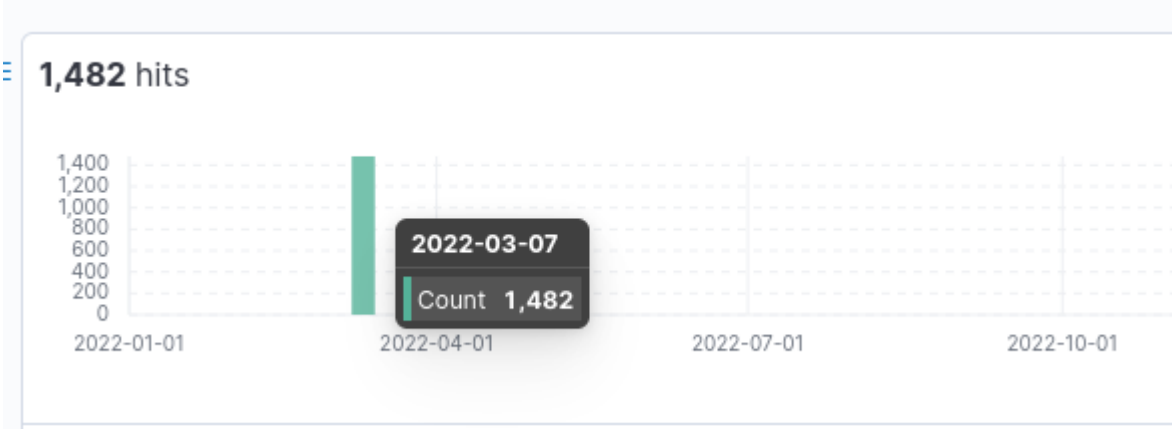

Figura 1 - Gráfico de eventos entre 01/01/2022 e 18/05/2024

Os dados aparentam começar em 7 de Março de 2022. Como sabemos que estamos falando de uma semana, colocarei a data inicial dia 6 de Março de 2022 por segurança, e a data final em 14 de Março de 2022.

Figura 2 - Gráfico de eventos entre 07/03/2022 e 14/03/2022

A Figura 2 nos mostra a mesma quantidade de hits da Figura 1, portanto conseguimos capturar todos os dados e eles se encontram entre 07/03/2022 e 12/03/2022. Essas informações nos permite responder a primeira pergunta da sala:

Quantos eventos foram retornados no mês de Março de 2022?

R: 1482

Agora, pelo contexto que nos foi dado, o usuário suspeito é Browne. Não é possível filtrar por usuários que iniciaram a comunicação, mas podemos começar pelos IPs de origem.

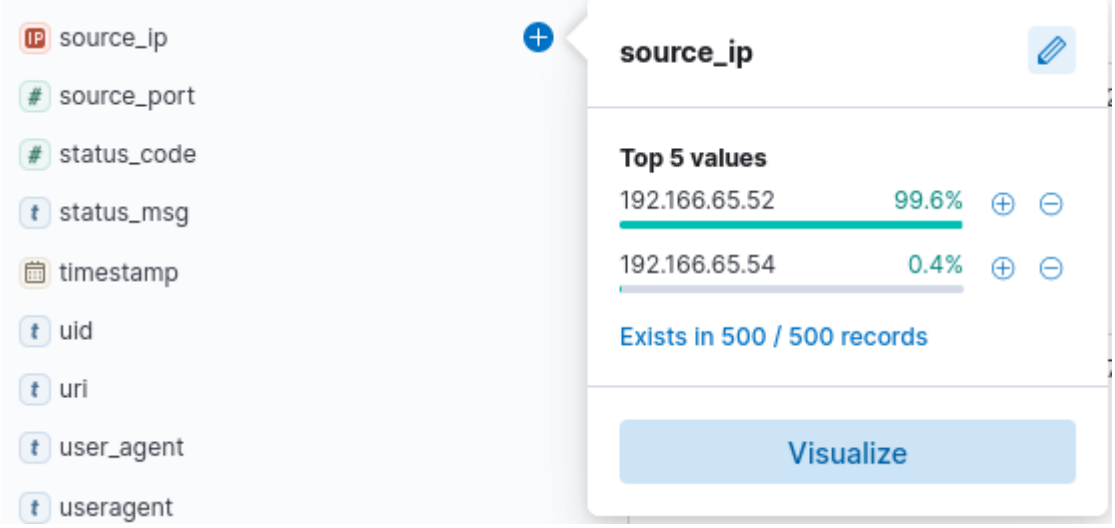

Figura 4 - Top 5 valores de IP de origem

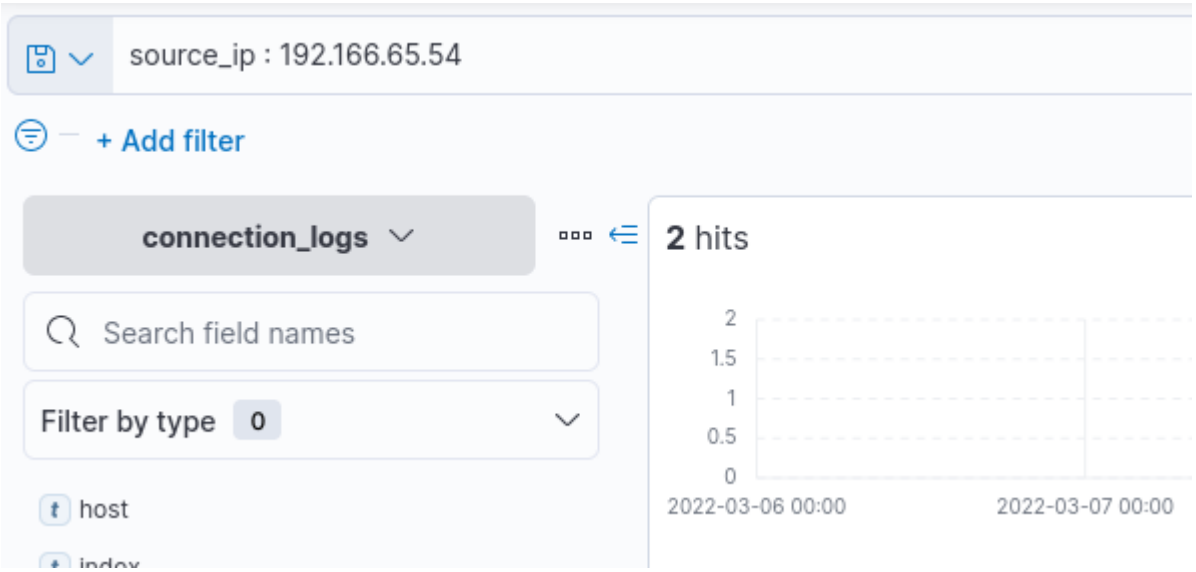

Figura 5 - Número de hits do IP 192.166.65.54

O IP 192.166.65.54 chama atenção por ter tido somente 2 conexões. Ao tentar responder a pergunta, vimos que fizemos a escolha correta.

Qual o IP associado com o usuário suspeito nos logs?

R: 192.166.65.54

Inspecionando o log, recebemos detalhes sobre como o usuário obteve os arquivos pelo parâmetro user_agent:

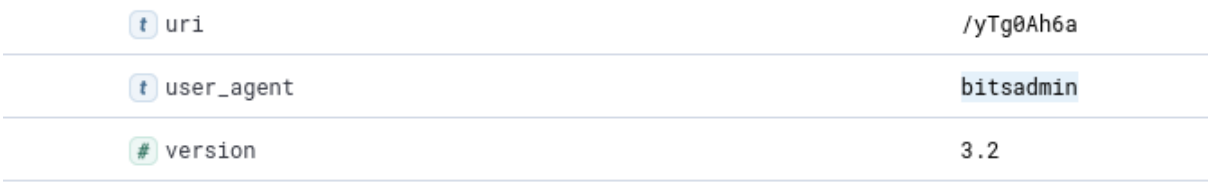

Figura 6a - Recorte 1 da análise de log de uma das comunicações do IP suspeito

A máquina do usuário usou um binário legítimo do windows para fazer download de arquivo de servidor C2. Qual o nome deste binário?

R: bitsadmin

Continuando nossa investigação, é possível ver o domínio e a página acessadas para obter o arquivo:

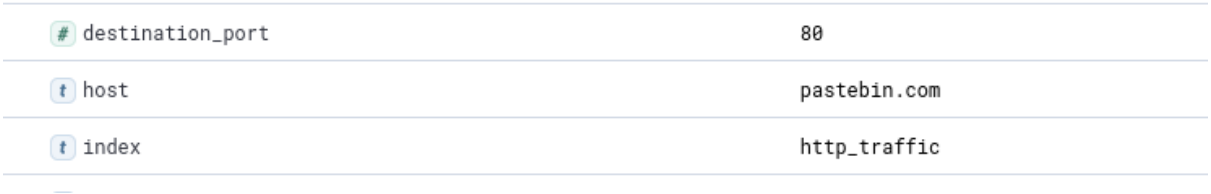

Figura 6b - Recorte 2 da análise de log de uma das comunicações do IP suspeito

A máquina infectada se conectou com um site de compartilhamento de arquivos famoso na época, que também age como servidor C2 pelos autores do malware para se comunicarem. Qual o nome deste site?

R: pastebin.com

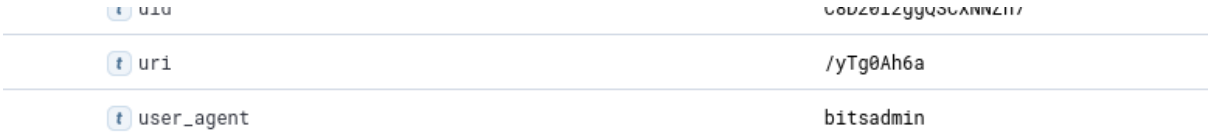

Figura 6c - Recorte 3 da análise de log de uma das comunicações do IP suspeito

Qual é a URL completa de C2 que o host infectado está conectado?

R: pastebin.com/yTg0Ah6a

Acessando o link pastebin, conseguimos encontrar a resposta para as duas últimas perguntas:

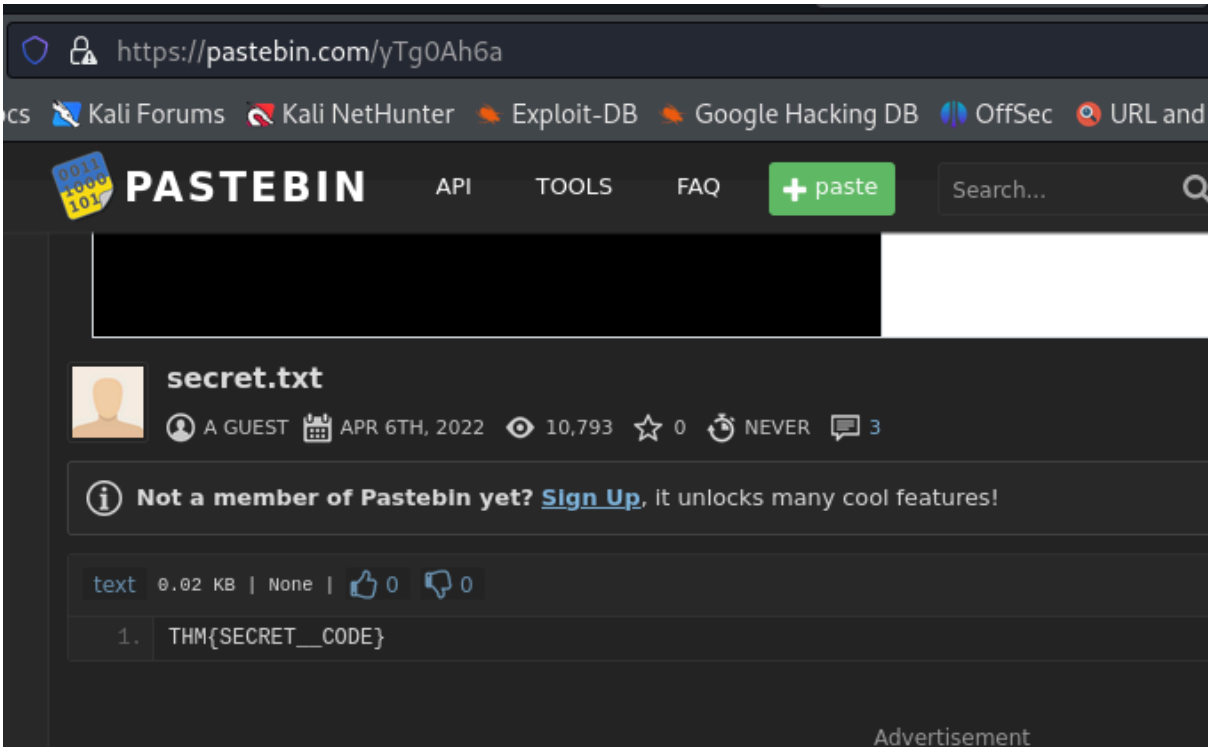

Figura 7 - Arquivo secreto no link do pastebin.com

Um arquivo foi acessado no site de compartilhamento. Qual o nome do arquivo acessado?

R: secret.txt

O arquivo contem um código secreto no formato THM{_____}.

R: {THM{SECRET__CODE}