Investigating with Splunk

Q1 How many events were collected and Ingested in the index main?

Use the query index=main
12256

Q2 On one of the infected hosts, the adversary was successful in creating a backdoor user. What is the new username?

Use the google to find the EventID of the user account creating which is 4720 and query that index=main EventID="4720"

```
ActivityID: {E0F7BC1B-4488-0000-8D57-1F92808AD601}
AllowedToDelegateTo: -
Category: User Account Management
Channel: Security
DisplayName: %%1793
EventID: 4720
EventReceivedTime: 2022-02-14 08:06:03
EventTime: 2022-02-14 08:06:02
EventType: AUDIT_SUCCESS
ExecutionProcessID: 740
HomeDirectory: %%1793
HomePath: %%1793
Hostname: Micheal.Beaven
Keywords: -9214364837600035000
LogonHours: %%1797
Message: A user account was created.

Subject:
        Security ID:            S-1-5-21-4020993649-1037605423-417876593-1104
        Account Name:           James
        Account Domain:         Cybertees
        Logon ID:               0x551686

New Account:
        Security ID:            S-1-5-21-1969843730-2406867588-1543852148-1000
        Account Name:           A1berto
        Account Domain:         WORKSTATION6
```

A1berto

Q3 On the same host, a registry key was also updated regarding the new backdoor user. What is the full path of that registry key?

I used the event id to find the log along with the hostname and the query is
index=main Micheal.Beaven EventID=13
HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto

Q4 Examine the logs and identify the user that the adversary was trying to impersonate.

The user name that we figured out is *A1berto* is similar to the name Alberto which is present in the user list in the left panel so the attacker is typing to mimic as the legitimate user
Alberto

Q5 What is the command used to add a backdoor user from a remote computer?

For this i used the EventId 4688 and the query is *index=main EventID=4688 "net user"*

C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1

Q6 How many times was the login attempt from the backdoor user observed during the investigation?

I used the Eventid for the both failed and successful login attempts from that user but no traces were there the EventId for Success 4624 and Failed is 4635
index=main A1berto EventID=4625
index=main A1berto EventID=4624
So the answer is zero (0)

Q7 What is the name of the infected host on which suspicious Powershell commands were executed?

We need to use the query used in the 5th question in order to find the hostname

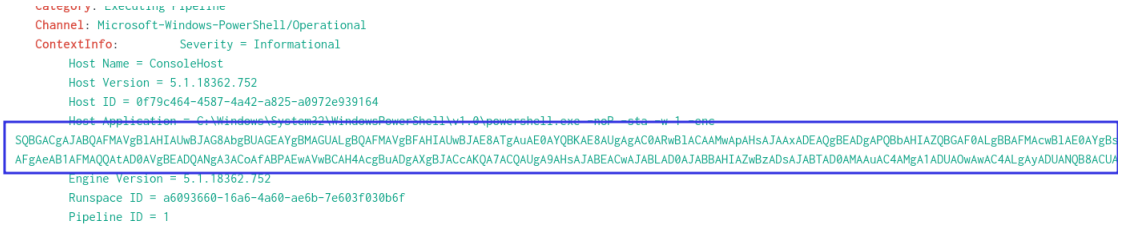
James.browne

Q8 PowerShell logging is enabled on this device. How many events were logged for the malicious PowerShell execution?

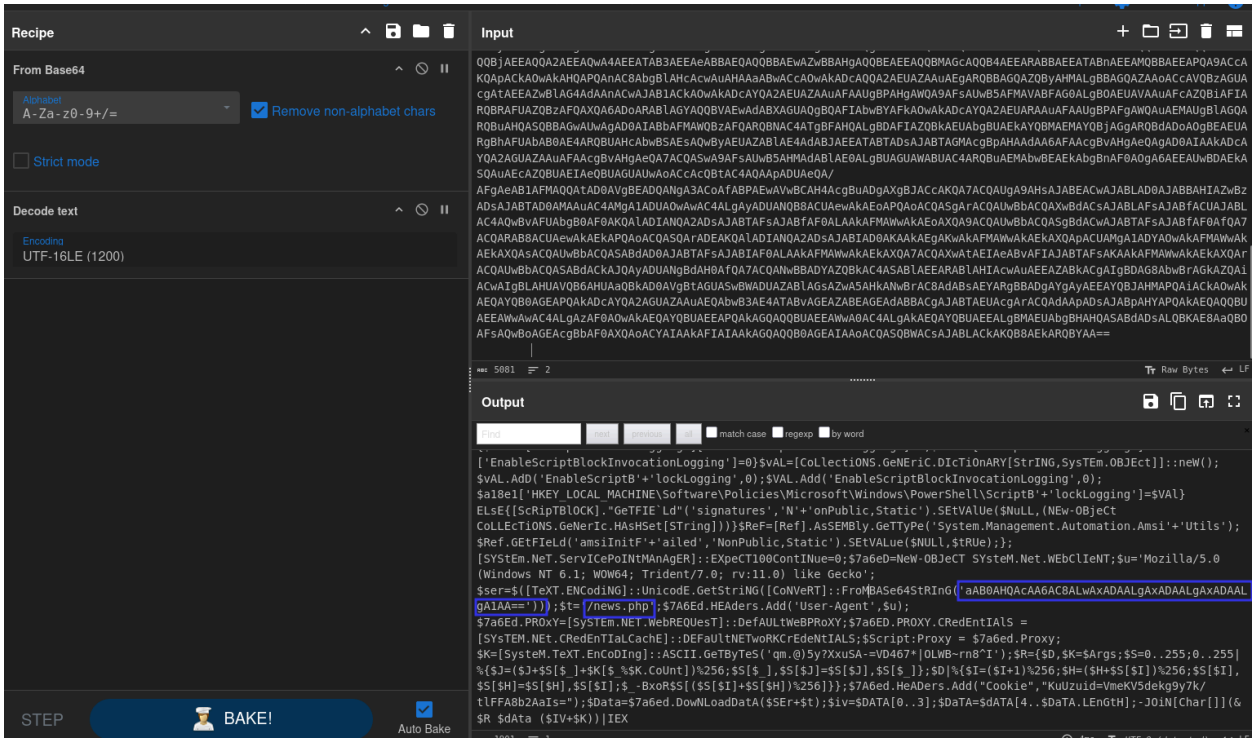
4103 or 4104 are the EventID for the powershell / cmd login
Use them to filter out
index=main EventID="4103"
79

Q9 An encoded Powershell script from the infected host initiated a web request. What is the full URL?

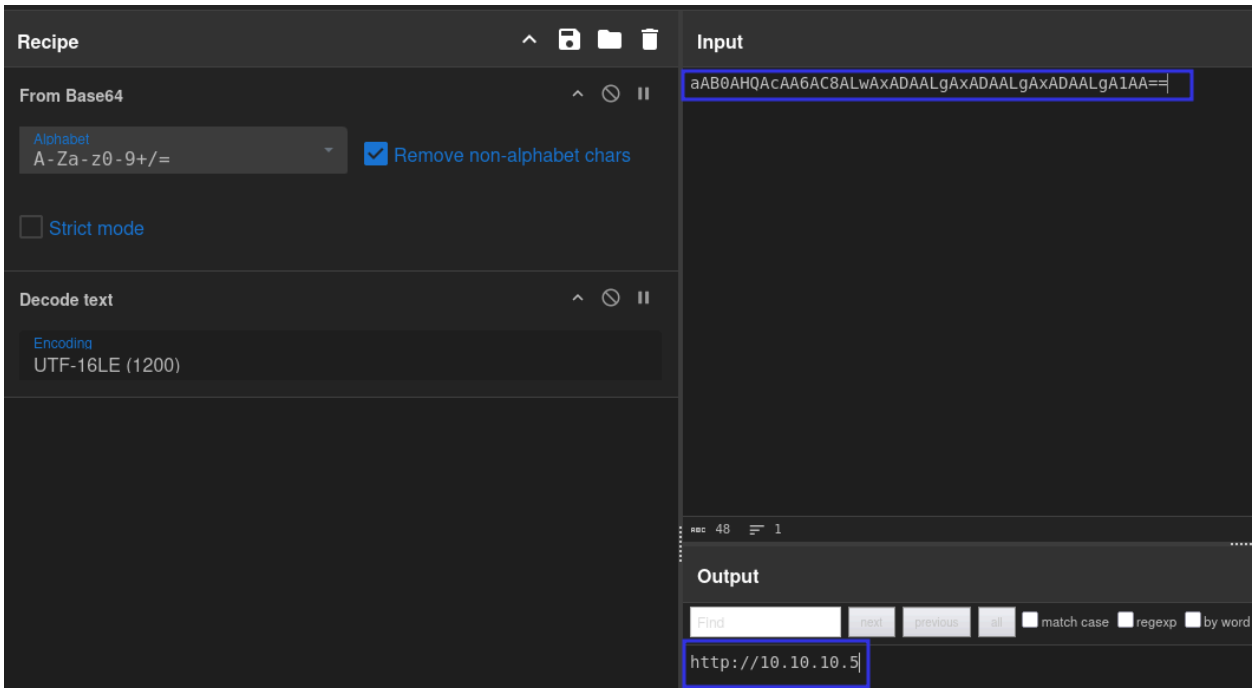
Use the logs of the previous question and get the encoded url and paste cyber chef , grab the url then defang it
First take take the complete encoded text



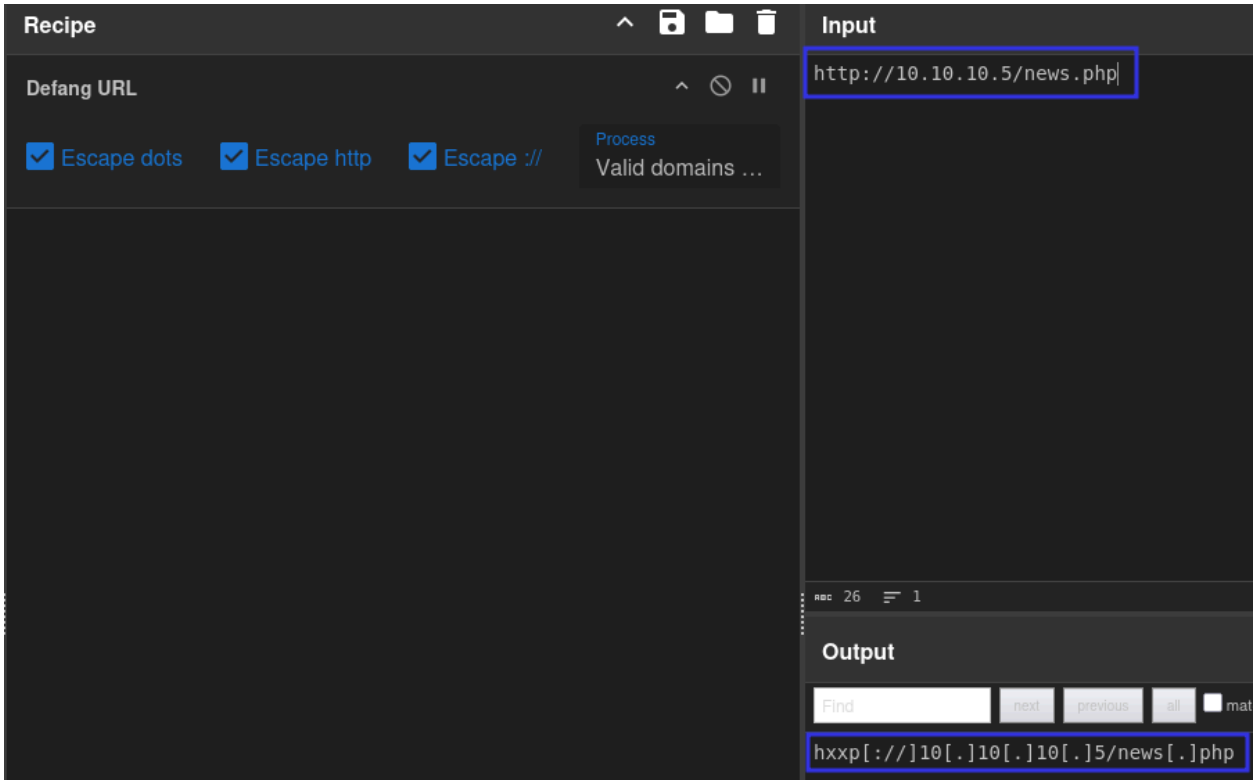
Then use cyber chef to decode this



Now take the base64 string again along to code this



and now add the /news.php to the url and use the defang url recipe



hxxp[://]10[.]10[.]10[.]5/news[.]php