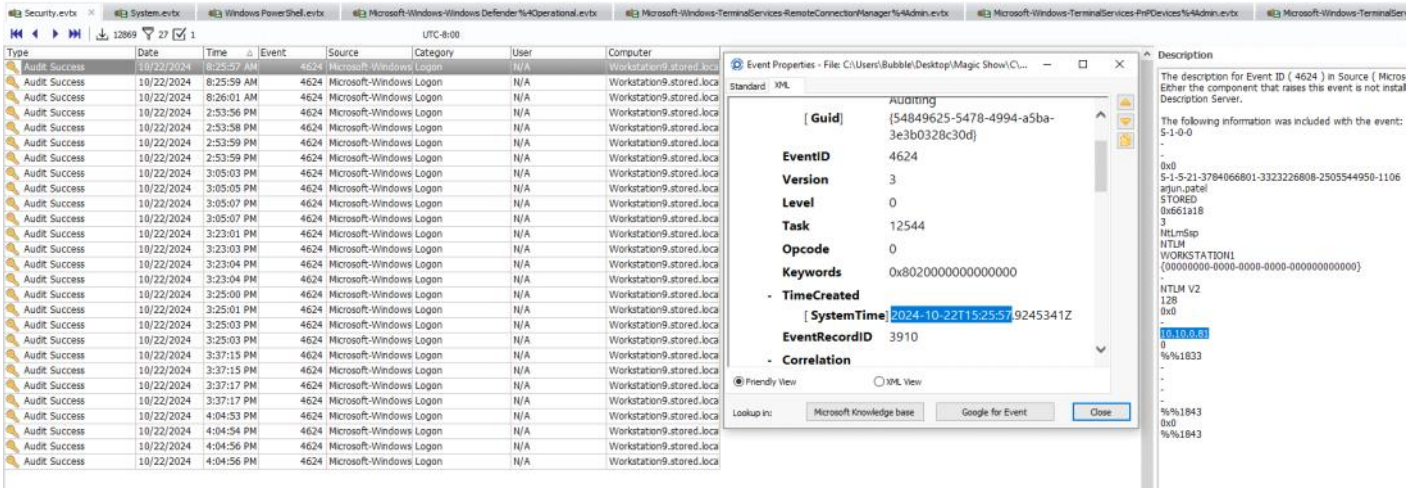
OpSalwarKameez24-2: Magic-Show

Sherlock Scenario
StoreD Technologies' System Administrators have observed several machines on the network unexpectedly rebooting to apply Windows updates during working hours. According to the organization's update policy, these updates should only occur overnight. As a member of StoreD Technologies' incident response team, your task is to investigate whether this unusual activity is linked to an ongoing security incident. System logs and a memory dump from one of the affected Windows 11 machines have been collected to assist in your investigation.

Task 1:
At What time did the compromised account first authenticate to the workstation? (UTC)

I searched for the IP 10.10.0.81 with event ID 4624 and it was the first event from the user arjun.patel.



Answer: 2024-10-22 15:25:57

Task 2:
What protocol did the threat actor us to access the workstation?

I answered this task first

While investigating the Security logs for event ID 4624 I saw several connections with logon type 10 (RDP) from IP 10.10.0.81

Answer: RDP

Task 3:
What logon type was logged when the threat actor accessed the workstation?

Same as previous task.

Answer: 10

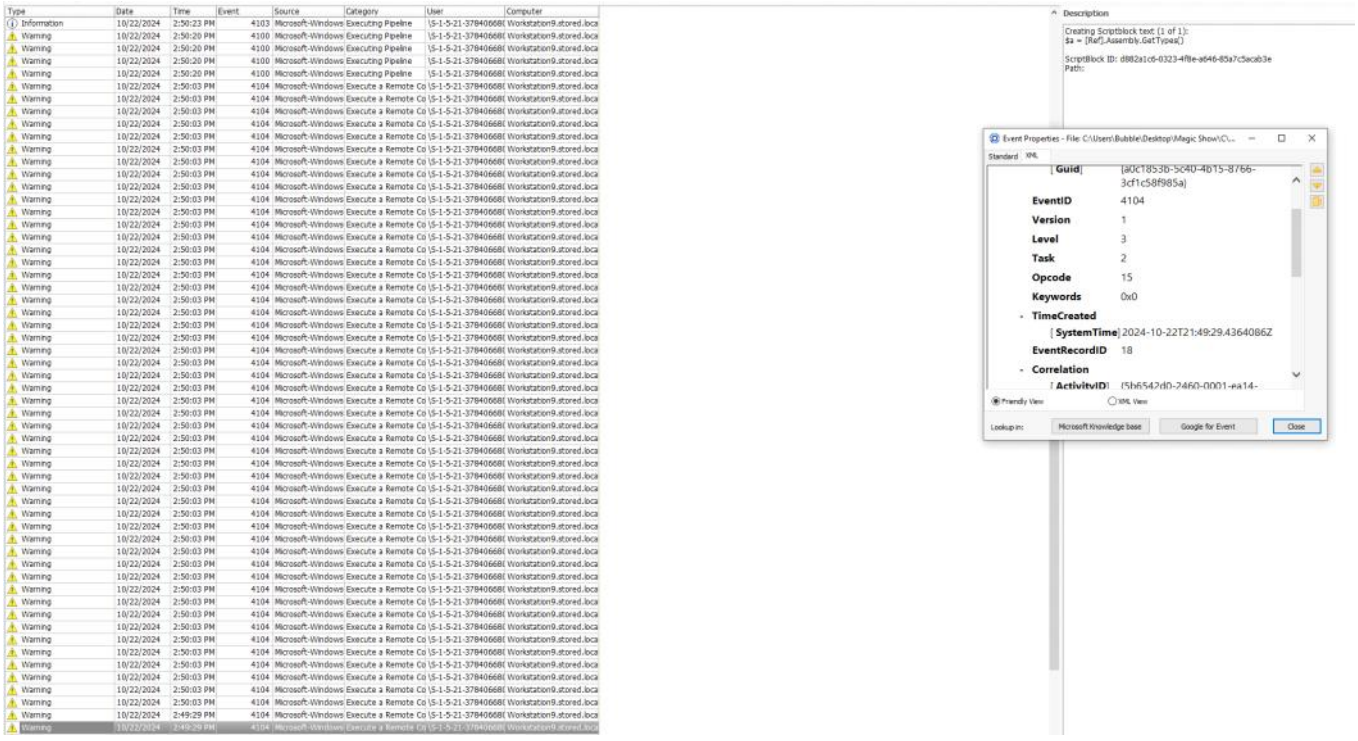
Task 4:
What was the IP address of the workstation the threat actor pivoted through to access the internal network?

Same as task 2

Answer: 10.10.0.81

Task 5:
At what time did the threat actor first attempt to bypass a feature of Windows Defender? (UTC)

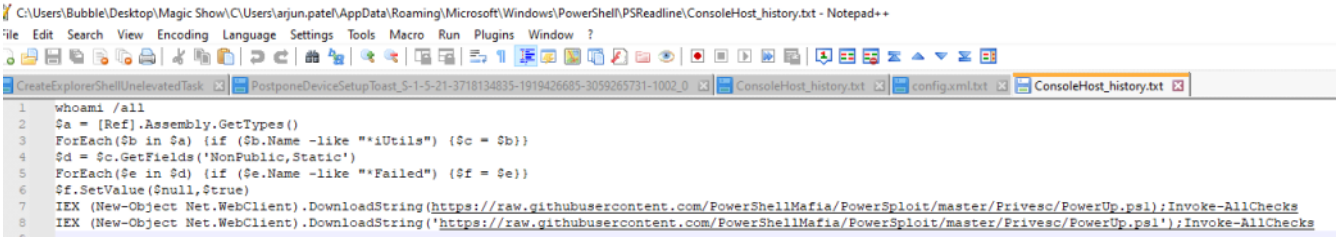
I searched the PowerShell operational and noticed the PowerUp script block so I went before the execution of the PowerUp and found the log



Answer: 2024-10-22 21:49:29

Task 6:
What is the name of the tool the threat actor used to enumerate the workstation for misconfigurations?

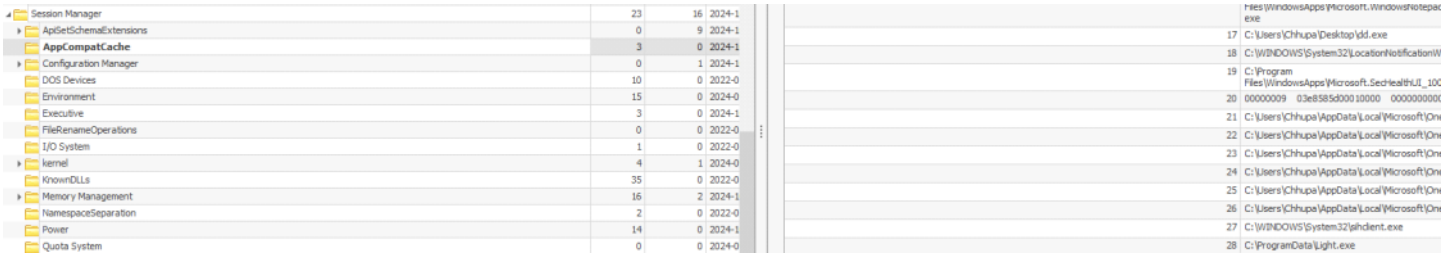
While checking the user arjun.patel files, I saw the PowerShell history and noticed the tool



Answer: PowerUp

Task 7:
What is the name of the executable the threat actor used to elevate their privileges?

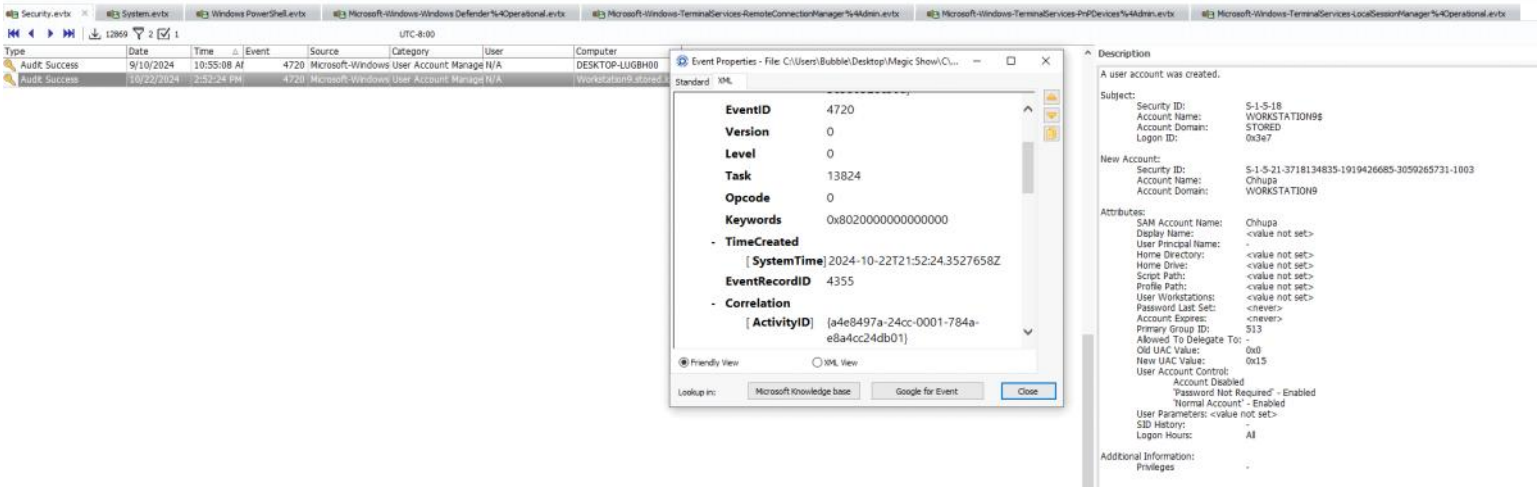
I checked the ShimCache from the path: SYSTEM\ControlSet00X\Control\Session Manager
\AppCompatCache to find for any executables and I saw some suspicious file from Program Data



Answer: light.exe

Task 8:
At what time did the new user get created? (UTC)

I searched for event ID 4720 and saw that the user is Chhupa which I already seen some malicious activity from him.



Answer: 2024-10-22 21:52:24

Task 9:
What was the SID of the user that created the new user?

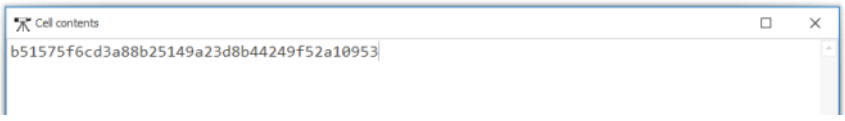
Same as previous task.
This SID is related to Local System account which is suspicious and might be related to the privilege escalation.

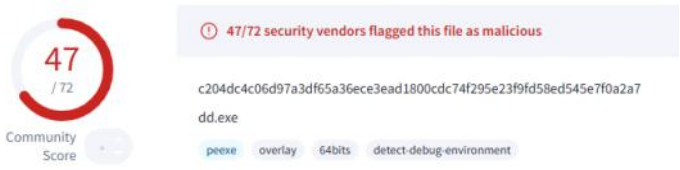
Answer: S-1-5-18

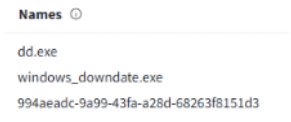
Task 10:
What is the original name of the exploit binary the threat actor used to bypass several Windows security features?

I checked for the executables inside Amcache and found the dd.exe with the SHA 1
b51575f6cd3a88b25149a23d8b44249f52a10953
I checked it on VirusTotal and checked the names in the details tab.

SHA1	Is Os Component	Full Path
b51575f6cd3a88b25149a23d8b44249f52a10953		c:\users\chhupa\desktop\dd.exe







Answer: windows_downdate.exe

Task 11:
What time did the threat actor first run the exploit? (UTC)

I searched for dd.exe

Previous Run2	Previous Run3	Previous Run4	Previous Run5	Previous Run6
=	=	=	=	=
2024-10-22 22:34:16	2024-10-22 22:33:59	2024-10-22 22:34:00	2024-10-22 22:31:43	2024-10-22 22:31:44

Answer: 2024-10-22 22:31:43

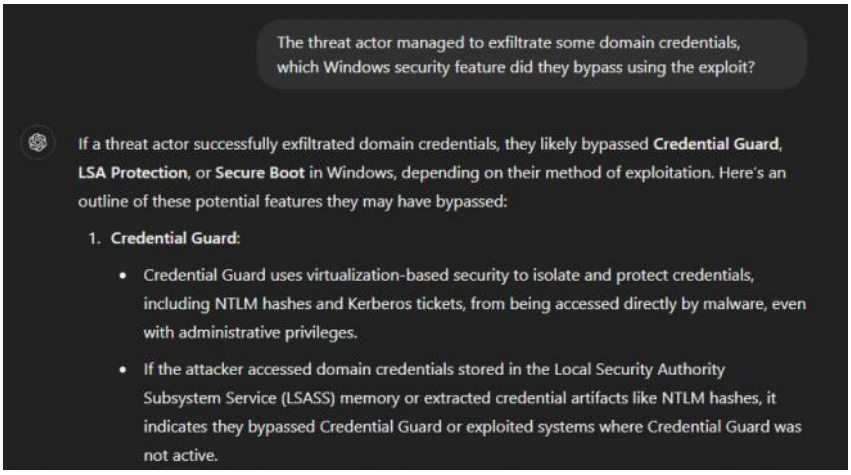
Task 12:
Which account owns the files manipulated by the exploit?

After checking with ChatGPT (Itamar)

Answer: TrustedInstaller

Task 13:
The threat actor managed to exfiltrate some domain credentials, which Windows security feature did they bypass using the exploit?

I asked the Chat



Answer: Credential Guard

Task 14:
What is the NT hash of the domain administrator compromised by the Threat Actor?

I used secretsdump.py to dump the hashes

'$DCC2$10240#Administrator#c7968e652be74a05e6e5e48826625bc6'

```
FLARE-VM Sun 12/01/2024  6:28:18.31
C:\Users\FlareVM\Desktop\mimikatz-master>python secretsdump.py -sam SAM -system SYSTEM -security SECURITY local
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[*] Target system bootKey: 0x1e8a03e19bbc807bccc804da7ce18217
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:7ad1d5a08c045d1d576f142fb13275b4:::
felamos:1001:aad3b435b51404eeaad3b435b51404ee:cf3a5525ee9414229e66279623ed5c58:::
badman:1002:aad3b435b51404eeaad3b435b51404ee:e72afd782e3d5c456d0a113acc298519:::
Chhupa:1003:aad3b435b51404eeaad3b435b51404ee:58a478135a93ac3bf058a5ea0e8fdb71:::
[*] Dumping cached domain logon information (domain/username:hash)
STORED.LOCAL/Administrator:$DCC2$10240#Administrator#c7968e652be74a05e6e5e48826625bc6: (2024-10-22 15:23:27)
STORED.LOCAL/aarush.roy:$DCC2$10240#aarush.roy#c227f8df681cf3529377a7f22da715ca: (2024-10-22 15:24:56)
STORED.LOCAL/arjun.patel:$DCC2$10240#arjun.patel#01e759109bba400d8679f0a235b2a39d: (2024-10-22 15:26:01)
[*] Dumping LSA Secrets
[*] $MACHINE.ACC
$MACHINE.ACC:plain_password_hex:3600630043004b007a00520050002200 6b0020002300330 05a004a0026003800610036002000270026002800 3d00580038003c003d00730021005f0047005f006b0041002000 6b0059003d005b006a004f002
d00510057005500 3a00450076007800330033003f0078006b003b002c00310075004d0043004100680025003500330036007 4002f004f0072004b0046003f0042005a00520029003900730060006300520041006000650050005900240 06d004f006c
005f00230044007500 6f00700068002300 2f0040002f00520050004900 2a003e0054004a0020003800 2c005b0071002e00290031007900 6f003a00
$MACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:a392843644741409925 38f192a219773
[*] DPAPI_SYSTEM
dpapi_machinekey:0xc93299b2213d09f2741fa125e0f409ab498acc43
dpapi_userkey:0xc8331d304da0cf525f9b72b2fd850a5ad5c7ad77
[-] LSA hashes extraction failed: read length must be non-negative or -1
[*] Cleaning up...

FLARE-VM Sun 12/01/2024  6:28:22.46
C:\Users\FlareVM\Desktop\mimikatz-master>
```

Then I used haschat to crack it

hashcat -m2100 '$DCC2$10240#Administrator#c7968e652be74a05e6e5e48826625bc6'
/usr/share/wordlists/rockyou.txt --force --potfile-disable

```
$DCC2$10240#administrator#c7968e652be74a05e6e5e48826625bc6:P@ssw0rd1

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 2100 (Domain Cached Credentials 2 (DCC2), MS Cache 2)
Hash.Target......: $DCC2$10240#administrator#c7968e652be74a05e6e5e48826625bc6
Time.Started.....: Sun Dec  1 09:45:25 2024, (59 secs)
Time.Estimated...: Sun Dec  1 09:46:24 2024, (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:     5461 H/s (8.95ms) @ Accel:64 Loops:1024 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 319488/14344385 (2.23%)
Rejected.........: 0/319488 (0.00%)
Restore.Point....: 318976/14344385 (2.22%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:9216-10239
Candidate.Engine.: Device Generator
Candidates.#1....: RAY123 -> LAWSON
Hardware.Mon.#1..: Util: 84%

Started: Sun Dec  1 09:44:43 2024
Stopped: Sun Dec  1 09:46:25 2024

┌──(root㉿kali)-[/usr/share/wordlists]
└─# hashcat -m2100 '$DCC2$10240#Administrator#c7968e652be74a05e6e5e48826625bc6' /usr/share/wordlists/rockyou.txt --force --potfile-disable
```

Then I converted the P@ssw0rd1 to NTLM

Answer: AE974876D974ABD805A989EBEAD86846

Task 15:
What is the password set by the threat actor for their generated user?

I used Mimikatz to dump the SAM, SYSTEM and SECURITY hives with the command:

lsadump::sam /sam:"C:\Users\Bubble\Desktop\SAM" /system:"C:\Users\Bubble\Desktop\SYSTEM" /security:"C:\Users\Bubble\Desktop\SECURITY"

Then I searched for the user Chhupa to copy his NTLM hash and use it on CrackStation

```
RID  : 000003eb (1003)
User : Chhupa
  Hash NTLM: 58a478135a93ac3bf058a5ea0e8fdb71
    lm  - 0: 008db196944de0b42a7e266d94e14826
    ntlm- 0: 58a478135a93ac3bf058a5ea0e8fdb71

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : 83e21c2c8fe079fb28980a50bf35efe2

* Primary:Kerberos-Newer-Keys *
    Default Salt : WORKSTATION9.STORED.LOCALChhupa
    Default Iterations : 4096
    Credentials
      aes256_hmac       (4096) : cb82bb90fdac8f63c5bb8392eceb7778558f4d5cc0c0e0fd853f95e858a96026
      aes128_hmac       (4096) : 539090e70014b19802e96a91e514293c
      des_cbc_md5       (4096) : d6b62c43a2cdc17c

* Packages *
    NTLM-Strong-NTOWF

* Primary:Kerberos *
    Default Salt : WORKSTATION9.STORED.LOCALChhupa
    Credentials
      des_cbc_md5       : d6b62c43a2cdc17c


mimikatz # lsadump::sam /sam:"C:\Users\Bubble\Desktop\SAM" /system:"C:\Users\Bubble\Desktop\SYSTEM" /security:"C:\Users\Bubble\Desktop\SECURITY"
```

✔ Found:

```
58a478135a93ac3bf058a5ea0e8fdb71:Password123
```

58a478135a93ac3bf058a5ea0e8fdb71

Answer: Password123