MEMORANDUM

To: Management

From: Team 03

Subject: Incident Report

Date: October 18, 2025

Summary: This report documents the actions of malicious actors within our systems and the steps taken to respond to these incidents and remediate the actions taken.

Team 03 would like to report evidence of a malicious actor in the domain controller attempting to move laterally through the network.

We identified that they were attempting to change remote code execution using psexec.exe.

Incident Details

Affected Host	Windows Server 2019 AD/DNS
Source IP Address	10.239.10.1
Destination IP Address	172.20.240.102
Port and Service	445/SMB (PsExec)
Initial Access Timestamp	1:44 PM CST
Service Downtime	None
Remediated Timestamp	1:55 PM CST
Affected Account	Administrator

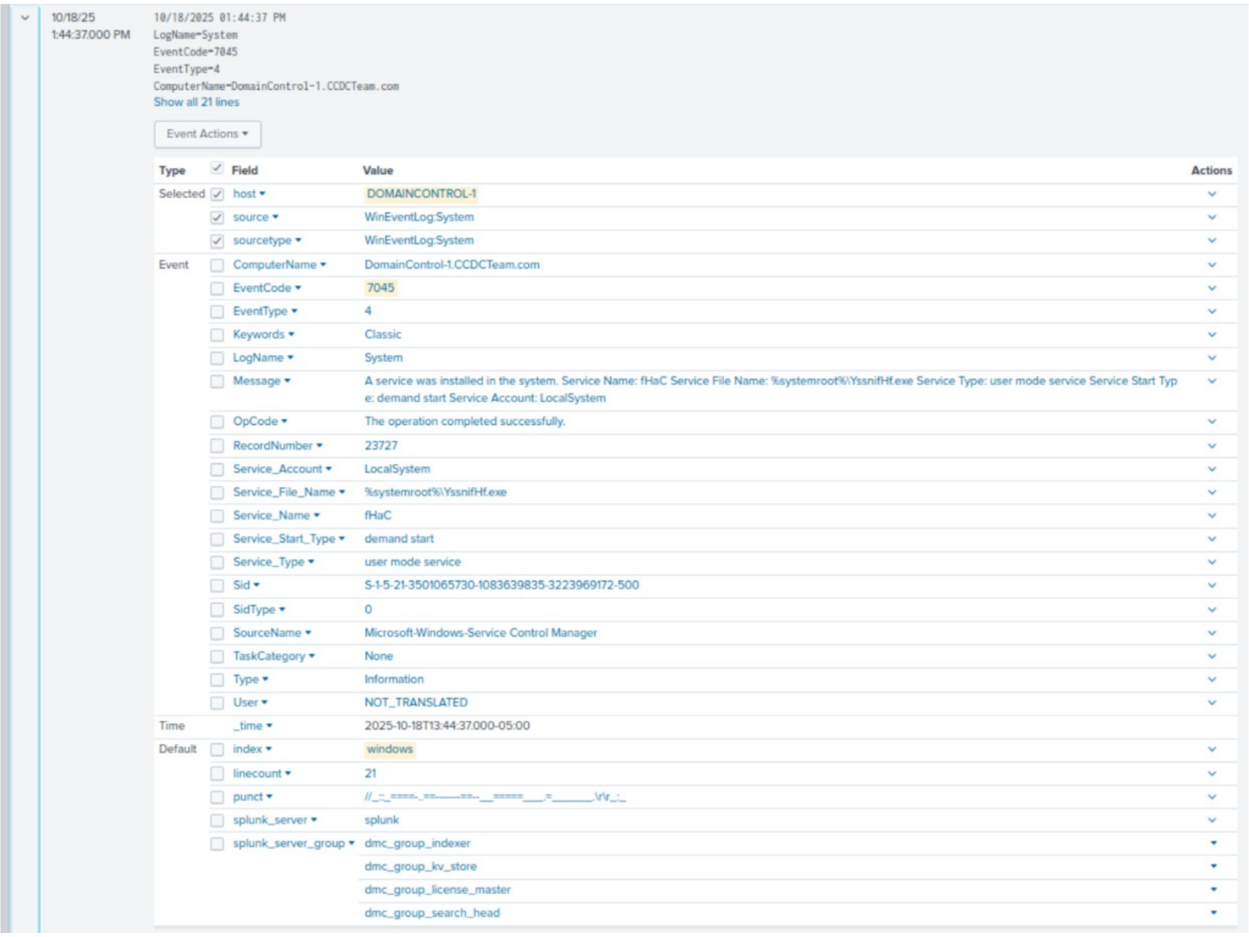
A malicious actor gained access to the company’s domain controller and attempted to achieve remote code execution using PsExec.exe in order to compromise the domain controller machine.

Vulnerability

The “Administrator” account had default, insecure, compromised credentials, and SMB was publicly accessible.

Initial Access

The attacker was able to login to the “Administrator” account with default credentials. Team 03 discovered this by using our Splunk indexer to look for service creation events on the domain controller (event code 7045), which are associated with PsExec, and then looking for remote login events (event code 4624) around the same time frame.



10/18/25
1:44:37.000 PM

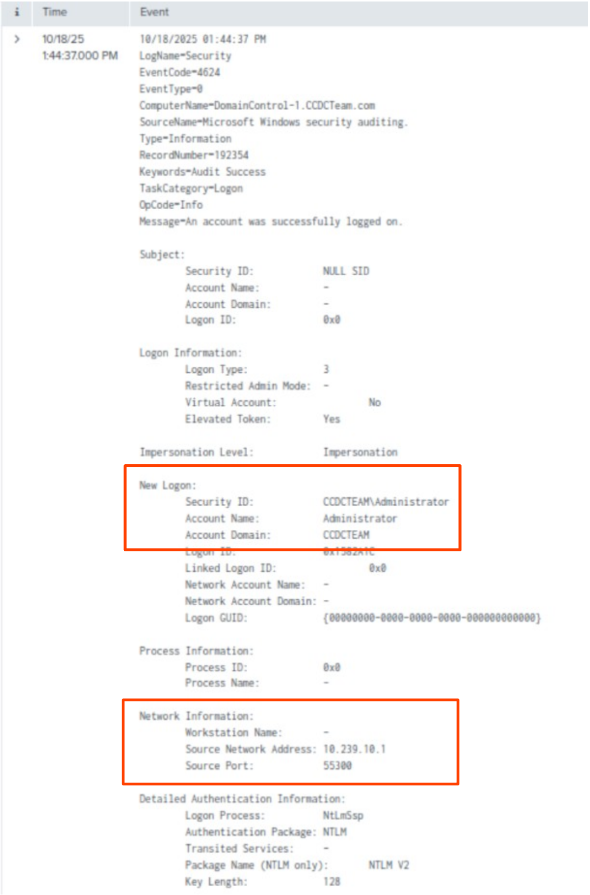
```
10/18/2025 01:44:37 PM
LogName=System
EventCode=7045
EventType=4
ComputerName=DomainControl-1.CCDCTeam.com
```

Show all 21 lines

Event Actions

Type	☑	Field	Value	Actions
Selected	☑	host	DOMAINCONTROL-1	⌄
	☑	source	WinEventLog:System	⌄
	☑	sourcetype	WinEventLog:System	⌄
Event	□	ComputerName	DomainControl-1.CCDCTeam.com	⌄
	□	EventCode	7045	⌄
	□	EventType	4	⌄
	□	Keywords	Classic	⌄
	□	LogName	System	⌄
	□	Message	A service was installed in the system. Service Name: fHaC Service File Name: %systemroot%\YssnifHf.exe Service Type: user mode service Service Start Typ e: demand start Service Account: LocalSystem	⌄
	□	OpCode	The operation completed successfully.	⌄
	□	RecordNumber	23727	⌄
	□	Service_Account	LocalSystem	⌄
	□	Service_File_Name	%systemroot%\YssnifHf.exe	⌄
	□	Service_Name	fHaC	⌄
	□	Service_Start_Type	demand start	⌄
	□	Service_Type	user mode service	⌄
	□	Sid	S-1-5-21-3501065730-1083639835-3223969172-500	⌄
	□	SidType	0	⌄
	□	SourceName	Microsoft-Windows-Service Control Manager	⌄
	□	TaskCategory	None	⌄
	□	Type	Information	⌄
	□	User	NOT_TRANSLATED	⌄
Time		_time	2025-10-18T13:44:37.000-05:00	
Default	□	index	windows	⌄
	□	linecount	21	⌄
	□	punct	//_:-_====-_==------==--__=====___-=_______\r\r_:_	⌄
	□	splunk_server	splunk	⌄
	□	splunk_server_group	dmc_group_indexer	▾
			dmc_group_kv_store	▾
			dmc_group_license_master	▾
			dmc_group_search_head	▾

Figure 1. Splunk search revealing malicious PsExec service creation (event code 7045)

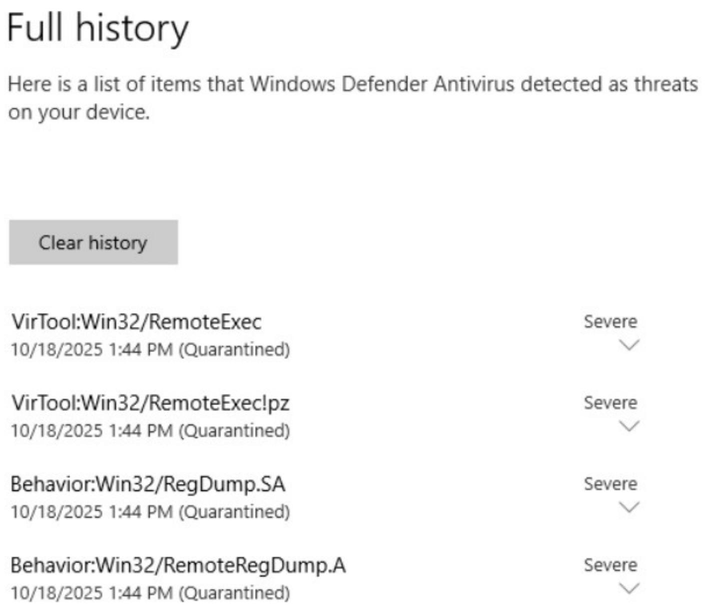


```
i   Time                 Event
>   10/18/25             10/18/2025 01:44:37 PM
    1:44:37.000 PM       LogName=Security
                         EventCode=4624
                         EventType=0
                         ComputerName=DomainControl-1.CCDCTeam.com
                         SourceName=Microsoft Windows security auditing.
                         Type=Information
                         RecordNumber=192354
                         Keywords=Audit Success
                         TaskCategory=Logon
                         OpCode=Info
                         Message=An account was successfully logged on.

                         Subject:
                                 Security ID:            NULL SID
                                 Account Name:           -
                                 Account Domain:         -
                                 Logon ID:               0x0

                         Logon Information:
                                 Logon Type:             3
                                 Restricted Admin Mode:  -
                                 Virtual Account:                No
                                 Elevated Token:         Yes

                         Impersonation Level:            Impersonation

                         New Logon:
                                 Security ID:            CCDCTEAM\Administrator
                                 Account Name:           Administrator
                                 Account Domain:         CCDCTEAM
                                 Logon ID:               0x1582A1C
                                 Linked Logon ID:                0x0
                                 Network Account Name:   -
                                 Network Account Domain: -
                                 Logon GUID:             {00000000-0000-0000-0000-000000000000}

                         Process Information:
                                 Process ID:             0x0
                                 Process Name:           -

                         Network Information:
                                 Workstation Name:       -
                                 Source Network Address: 10.239.10.1
                                 Source Port:            55300

                         Detailed Authentication Information:
                                 Logon Process:          NtLmSsp
                                 Authentication Package: NTLM
                                 Transited Services:     -
                                 Package Name (NTLM only):       NTLM V2
                                 Key Length:             128
```

Figure 2. Login to user “Administrator” from remote IP (10.239.10.1)

Impact

Team 03 was able to catch the malicious access to our systems and as a result was able to prevent any impact to our business services. Windows Defender caught and stopped their attempts to use PsExec to execute malicious commands by quarantining their execution scripts, which alerted us to their activity.



Full history

Here is a list of items that Windows Defender Antivirus detected as threats on your device.

VirTool:Win32/RemoteExec
10/18/2025 1:44 PM (Quarantined) Severe

VirTool:Win32/RemoteExec!pz
10/18/2025 1:44 PM (Quarantined) Severe

Behavior:Win32/RegDump.SA
10/18/2025 1:44 PM (Quarantined) Severe

Behavior:Win32/RemoteRegDump.A
10/18/2025 1:44 PM (Quarantined) Severe

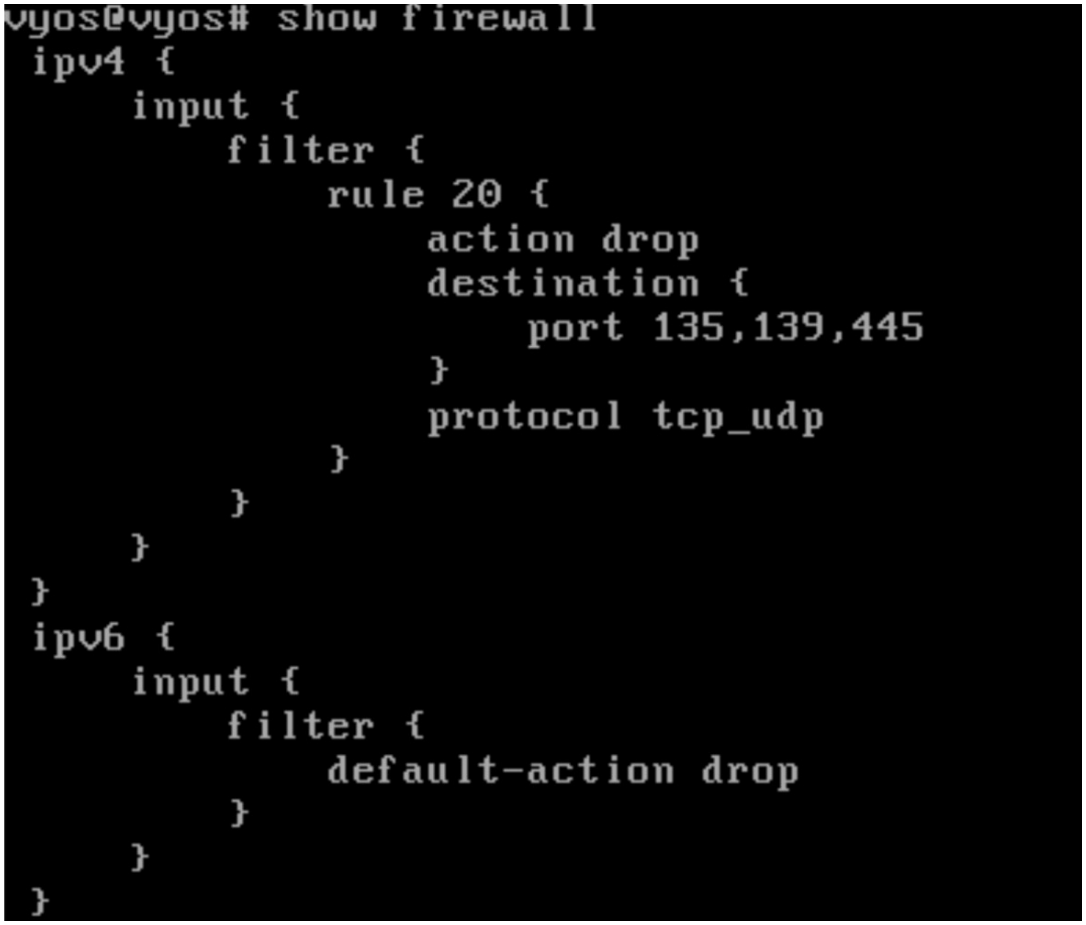
Figure 3. Windows Defender Antivirus threat detected.

Eradication

The account used by the malicious actor “Administrator” was disabled by Team 03.

Remediation

Team 03 blocked SMB ports 445 and 139 along with the Remote Procedure Call port 135 on the VyOS Router.



```
vyos@vyos# show firewall
 ipv4 {
     input {
         filter {
             rule 20 {
                 action drop
                 destination {
                     port 135,139,445
                 }
                 protocol tcp_udp
             }
         }
     }
 }
 ipv6 {
     input {
         filter {
             default-action drop
         }
     }
 }
```

Figure 4. Firewall rules on VyOS.

If there are any other questions about this incident, please do not hesitate to reach out and Team 03 would be happy to provide more information.

Thank you,
Team 03