Pre-Ransomware Behavioral Detection & Incident Response

Using Sysmon Telemetry and Elastic SIEM

Author: Vatsal Saxena

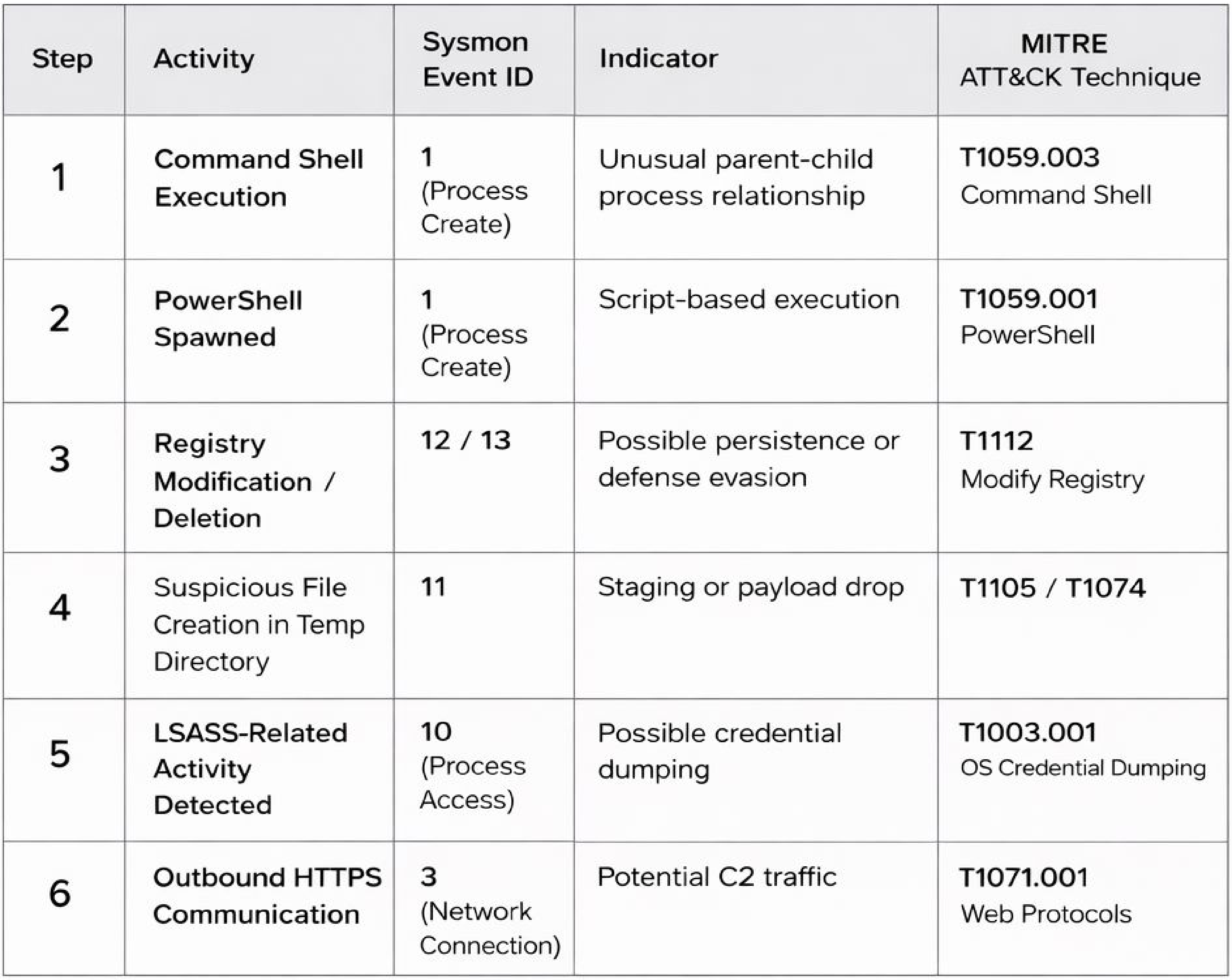
Project Type: SOC Analyst Detection Engineering Lab

1. Executive Summary

This project focuses on detecting pre-ransomware behavioral activity using Windows Sysmon logs integrated into Elastic SIEM. Instead of relying on signature-based detection, this approach identifies suspicious behavioral patterns such as PowerShell execution, registry manipulation, LSASS interaction, file staging, and outbound command-and-control communication.

Through multi-event correlation, this project demonstrates how early-stage ransomware indicators can be detected before encryption begins, enabling proactive incident response.

Multi-Event Correlation Analysis



Step	Activity	Sysmon Event ID	Indicator	MITRE ATT&CK Technique
1	**Command Shell Execution**	1 (Process Create)	Unusual parent-child process relationship	T1059.003 Command Shell
2	**PowerShell Spawned**	1 (Process Create)	Script-based execution	T1059.001 PowerShell
3	**Registry Modification / Deletion**	12 / 13	Possible persistence or defense evasion	T1112 Modify Registry
4	Suspicious File Creation in Temp Directory	11	Staging or payload drop	T1105 / T1074
5	**LSASS-Related Activity Detected**	10 (Process Access)	Possible credential dumping	T1003.001 OS Credential Dumping
6	**Outbound HTTPS Communication**	3 (Network Connection)	Potential C2 traffic	T1071.001 Web Protocols

Attack Timeline Reconstruction

Stage	Technical Observation
Execution	'**cmd.exe**' spawned '**powershell.exe**' (Sysmon EID 1) within short time window indicating script-based execution
Persistence	Registry '**RunOnce**' key modification detected (Sysmon EID **12/13**) suggesting potential startup persistence
Credential Access	**LSASS process access observed (Sysmon EID 10**) indicating possible credential dumping attempt
Staging	Suspicious file created in Temp directory (Sysmon EID 11), likely payload staging
Command & Control	Outbound TCP 443 connection initiated (Sysmon EID 3), potential encrypted C2 communication
	Outbound TCP **443 connection** initiated (Sysmon EID 3), potential encrypted C2 communication

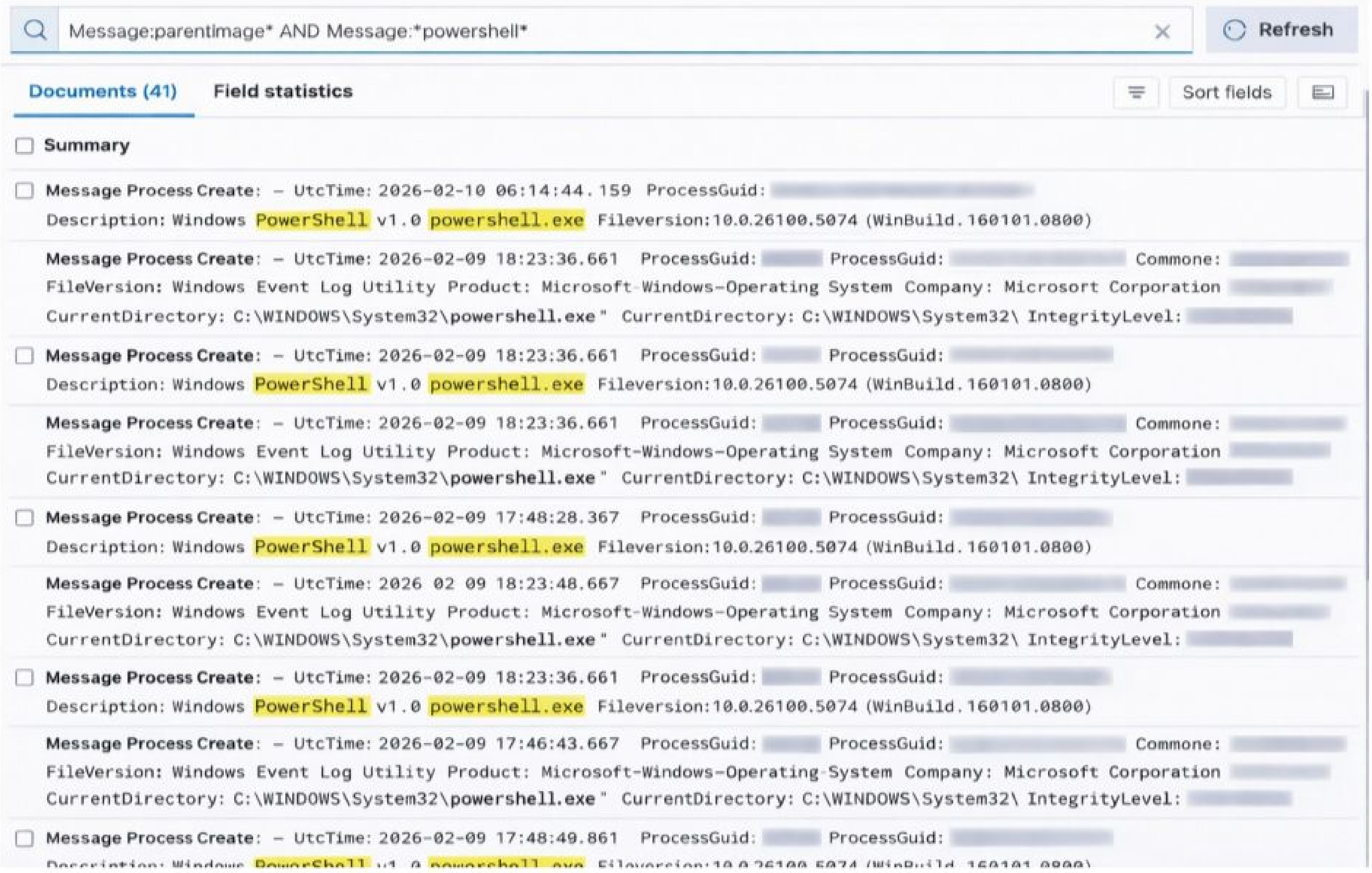
1. Parent-Child Process Analysis (cmd.exe → PowerShell)

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
Message:parentimage* AND Message:*powershell*
```

```
☐ Message Process Create: – UtcTime: 2026-02-10 06:14:44.159 ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild.160101.0800)
  Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating System Company: Microsort Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
☐ Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild.160101.0800)
  Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating System Company: Microsoft Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
☐ Message Process Create: – UtcTime: 2026-02-09 17:48:28.367  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild.160101.0800)
  Message Process Create: – UtcTime: 2026 02 09 18:23:48.667  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating System Company: Microsoft Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
☐ Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild.160101.0800)
  Message Process Create: – UtcTime: 2026-02-09 17:46:43.667  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating-System Company: Microsoft Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
☐ Message Process Create: – UtcTime: 2026-02-09 17:48:49.861  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild.160101.0800)
```

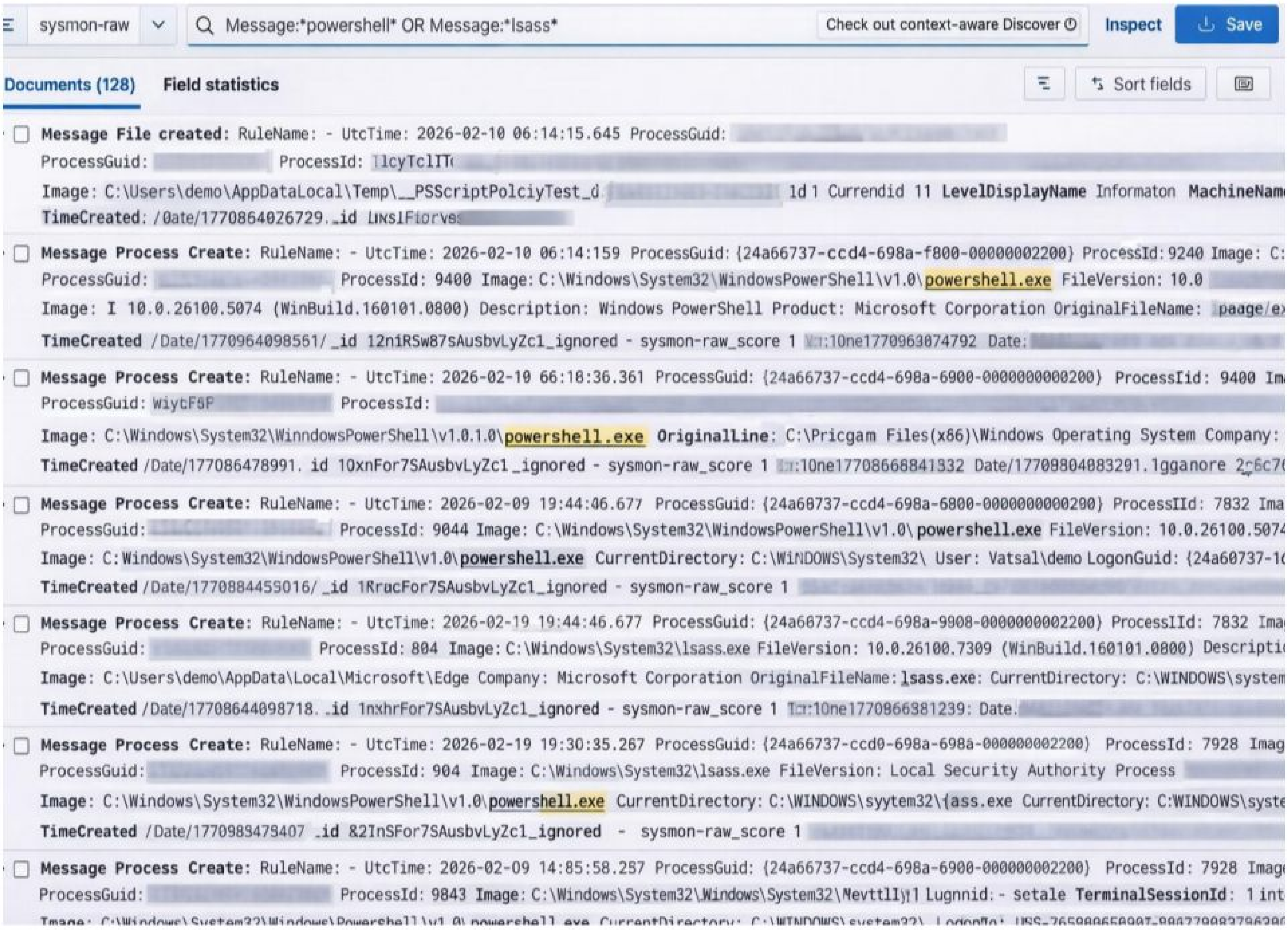
2. PowerShell and LSASS Behavioral Detection

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
Message:*powershell* OR Message:*lsass*
```

```
□ Message File created: RuleName: - UtcTime: 2026-02-10 06:14:15.645 ProcessGuid: [redacted]
  ProcessGuid: [redacted] ProcessId: 1lcyTclIT[redacted]
  Image: C:\Users\demo\AppDataLocal\Temp\__PSScriptPolciyTest_d[redacted] 1d 1 Currendid 11 LevelDisplayName Informaton MachineNam
  TimeCreated: /0ate/1770864026729._id LINSlFiorve[redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:14:159 ProcessGuid:{24a66737-ccd4-698a-f800-00000002200} ProcessId:9240 Image: C:
  ProcessGuid: [redacted] ProcessId: 9400 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0 [redacted]
  Image: I 10.0.26100.5074 (WinBuild.160101.0800) Description: Windows PowerShell Product: Microsoft Corporation OriginalFileName: paage/ex
  TimeCreated /Date/1770964098561/_id 12n1RSw87sAusbvLyZc1_ignored - sysmon-raw_score 1 :10ne1770963074792 Date:[redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-10 66:18:36.361 ProcessGuid: {24a66737-ccd4-698a-6900-0000000000200} ProcessIid: 9400 Im
  ProcessGuid: WiytF6P[redacted] ProcessId: [redacted]
  Image: C:\Windows\System32\WinndowsPowerShell\v1.0.1.0\powershell.exe OriginalLine: C:\Pricgam Files(x86)\Windows Operating System Company:
  TimeCreated /Date/177086478991. id 10xnFor7SAusbvLyZc1_ignored - sysmon-raw_score 1 :10ne17708668841332 Date/17708804083291.1gganore 2c6c7

□ Message Process Create: RuleName: - UtcTime: 2026-02-09 19:44:46.677 ProcessGuid: {24a60737-ccd4-698a-6800-0000000000290} ProcessIId: 7832 Ima
  ProcessGuid: [redacted] ProcessId: 9044 Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0.26100.507
  Image: C:Windows\System32\WindowsPowerShell\v1.0\powershell.exe CurrentDirectory: C:\WiNDOWS\System32\ User: Vatsal\demo LogonGuid: {24a60737-1
  TimeCreated /Date/1770884459016/_id 1RrucFor7SAusbvLyZc1_ignored - sysmon-raw_score 1 [redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-19 19:44:46.677 ProcessGuid: {24a66737-ccd4-698a-9908-0000000002200} ProcessIId: 7832 Ima
  ProcessGuid: [redacted] ProcessId: 804 Image: C:\Windows\System32\lsass.exe FileVersion: 10.0.26100.7309 (WinBuild.160101.0800) Descripti
  Image: C:\Users\demo\AppData\Local\Microsoft\Edge Company: Microsoft Corporation OriginalFileName: lsass.exe: CurrentDirectory: C:\WINDOWS\system
  TimeCreated /Date/17708644098718. _id 1nxhrFor7SAusbvLyZc1_ignored - sysmon-raw_score 1 T:10ne1770866381239: Date.[redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-19 19:30:35.267 ProcessGuid: {24a66737-ccd0-698a-698a-000000002200) ProcessId: 7928 Imag
  ProcessGuid: [redacted] ProcessId: 904 Image: C:\Windows\System32\lsass.exe FileVersion: Local Security Authority Process [redacted]
  Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe CurrentDirectory: C:\WINDOWS\syytem32\{ass.exe CurrentDirectory: C:WINDOWS\syste
  TimeCreated /Date/1770983479407 _id &2InSFor7SAusbvLyZc1_ignored - sysmon-raw_score 1 [redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-09 14:85:58.257 ProcessGuid: {24a66737-ccd4-698a-6900-000000002200) ProcessId: 7928 Imag
  ProcessGuid: [redacted] ProcessId: 9843 Image: C:\Windows\System32\Windows\System32\Mevttll1 Lugnnid: - setale TerminalSessionId: 1 int
  Image: C:\Windows\System32\Windows\Powershell\v1.0\powershell.exe CurrentDirectory: C:\WINDOWS\system32\ LogonId: US-765990659907-99477998379639
```

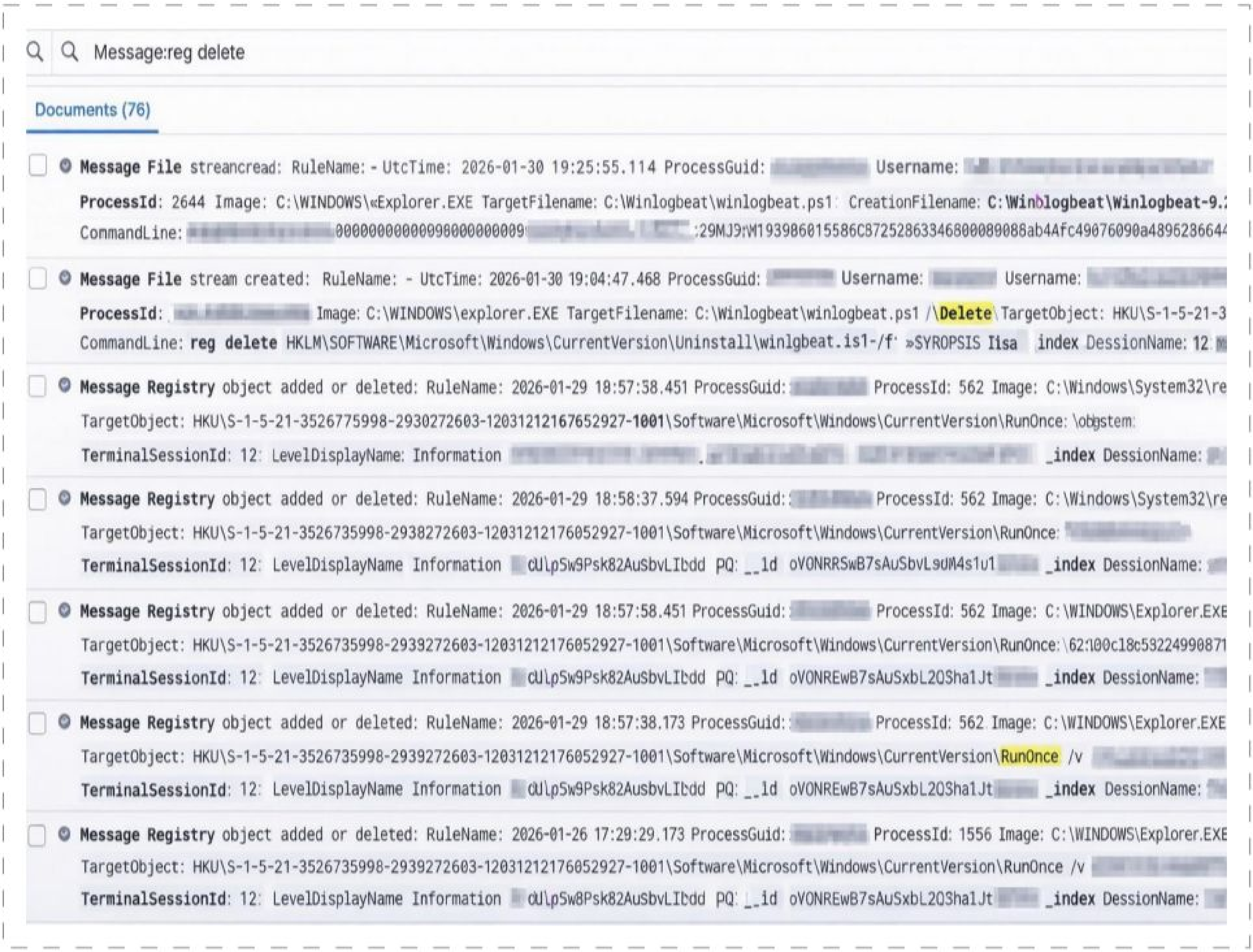
3. Registry Deletion Activity (Persistence Tampering)

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



Message:reg delete

Documents (76)

```
□ ● Message File streancread: RuleName: - UtcTime: 2026-01-30 19:25:55.114 ProcessGuid: [redacted] Username: [redacted]
    ProcessId: 2644 Image: C:\WINDOWS\«Explorer.EXE TargetFilename: C:\Winlogbeat\winlogbeat.ps1  CreationFilename: C:\Winblogbeat\Winlogbeat-9.
    CommandLine: [redacted] 000000000000980000000009 [redacted] :29MJ9:M193986015586C87252863346800089088ab4Afc49076090a489628664

□ ● Message File stream created:  RuleName: - UtcTime: 2026-01-30 19:04:47.468 ProcessGuid: [redacted] Username: [redacted] Username: [redacted]
    ProcessId: [redacted] Image: C:\WINDOWS\explorer.EXE TargetFilename: C:\Winlogbeat\winlogbeat.ps1 /\Delete\ TargetObject: HKU\S-1-5-21-3
    CommandLine: reg delete HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\winlgbeat.is1-/f' »SYROPSIS Iisa  index DessionName: 12 [redacted]

□ ● Message Registry object added or deleted: RuleName: 2026-01-29 18:57:58.451 ProcessGuid: [redacted] ProcessId: 562 Image: C:\Windows\System32\re
    TargetObject: HKU\S-1-5-21-3526775998-2930272603-12031212167652927-1001\Software\Microsoft\Windows\CurrentVersion\RunOnce: \obgstem:
    TerminalSessionId: 12: LevelDisplayName: Information [redacted] _index DessionName: [redacted]

□ ● Message Registry object added or deleted: RuleName: 2026-01-29 18:58:37.594 ProcessGuid: [redacted] ProcessId: 562 Image: C:\Windows\System32\re
    TargetObject: HKU\S-1-5-21-3526735998-2938272603-12031212176052927-1001\Software\Microsoft\Windows\CurrentVersion\RunOnce: [redacted]
    TerminalSessionId: 12: LevelDisplayName Information [redacted] cUlp5w9Psk82AuSbvLIbdd PQ: __ld oVONRRSwB7sAuSbvL9UM4s1u1 [redacted] _index DessionName: [redacted]

□ ● Message Registry object added or deleted: RuleName: 2026-01-29 18:57:58.451 ProcessGuid: [redacted] ProcessId: 562 Image: C:\WINDOWS\Explorer.EXE
    TargetObject: HKU\S-1-5-21-3526735998-2939272603-12031212176052927-1001\Software\Microsoft\Windows\CurrentVersion\RunOnce: \62:100c18c53224990871
    TerminalSessionId: 12: LevelDisplayName Information [redacted] cUlp5w9Psk82AuSbvLIbdd PQ: __ld oVONREwB7sAuSxbL2QSha1Jt [redacted] _index DessionName: [redacted]

□ ● Message Registry object added or deleted: RuleName: 2026-01-29 18:57:38.173 ProcessGuid: [redacted] ProcessId: 562 Image: C:\WINDOWS\Explorer.EXE
    TargetObject: HKU\S-1-5-21-3526735998-2939272603-12031212176052927-1001\Software\Microsoft\Windows\CurrentVersion\RunOnce /v [redacted]
    TerminalSessionId: 12: LevelDisplayName Information [redacted] cUlp5w9Psk82AusbvLIbdd PQ: __ld oVONREwB7sAuSxbL2QSha1Jt [redacted] _index DessionName: [redacted]

□ ● Message Registry object added or deleted: RuleName: 2026-01-26 17:29:29.173 ProcessGuid: [redacted] ProcessId: 1556 Image: C:\WINDOWS\Explorer.EXE
    TargetObject: HKU\S-1-5-21-3526735998-2939272603-12031212176052927-1001\Software\Microsoft\Windows\CurrentVersion\RunOnce /v [redacted]
    TerminalSessionId: 12: LevelDisplayName Information [redacted] cUlp5w8Psk82AuSbvLIbdd PQ: __ld oVONREwB7sAuSxbL2QSha1Jt [redacted] _index DessionName: [redacted]
```

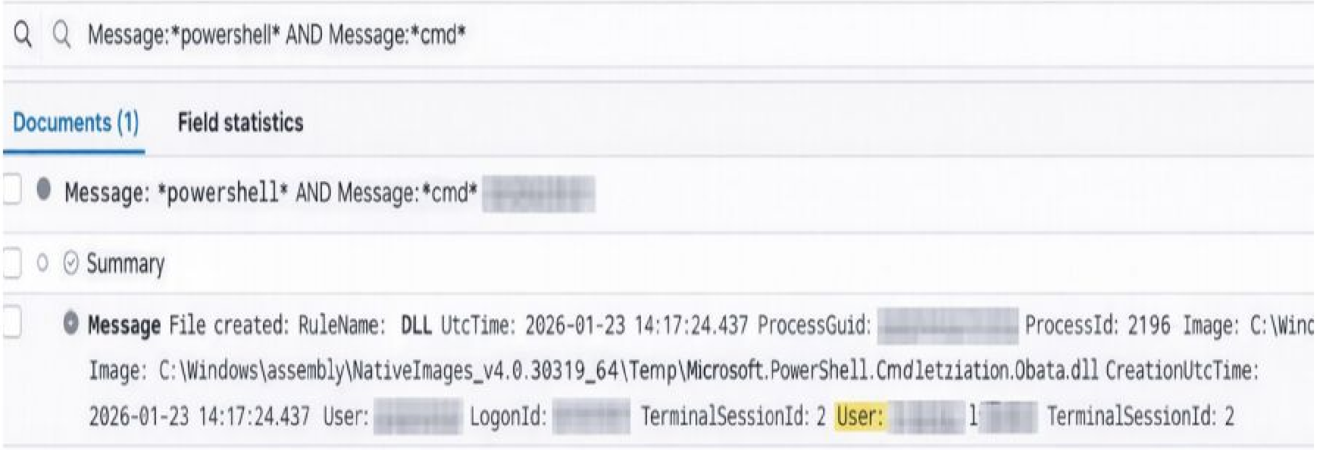
4. Command Chaining (PowerShell + CMD Correlation)

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
Message: *powershell* AND Message:*cmd* [redacted]
Summary
Message File created: RuleName:  DLL UtcTime: 2026-01-23 14:17:24.437 ProcessGuid: [redacted] ProcessId: 2196 Image: C:\Winc
Image: C:\Windows\assembly\NativeImages_v4.0.30319_64\Temp\Microsoft.PowerShell.Cmdletziation.Obata.dll CreationUtcTime:
2026-01-23 14:17:24.437 User: [redacted] LogonId: [redacted] TerminalSessionId: 2 User: [redacted] 1[redacted] TerminalSessionId: 2
```

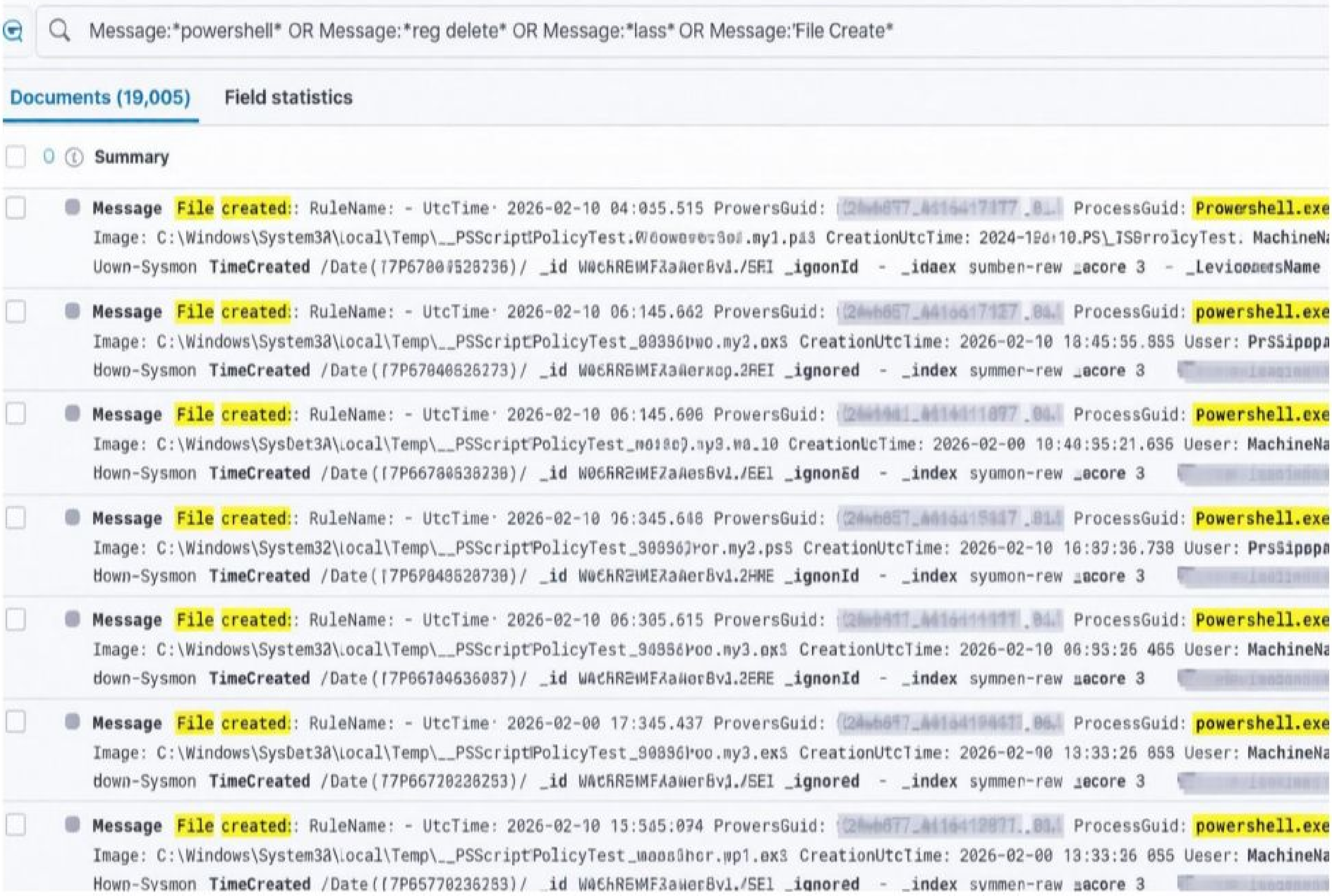
5. Broad Multi-Indicator Behavioral Query

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



Message:*powershell* OR Message:*reg delete* OR Message:*lass* OR Message:'File Create*

```
Message File created:: RuleName: - UtcTime· 2026-02-10 04:035.515 ProwersGuid: [redacted] ProcessGuid: Prowershell.exe
Image: C:\Windows\System3A\local\Temp\__PSScriptPolicyTest.W6owe9e:8o#.my1.pa3 CreationUtcTime: 2024-19a:10.PS\_ISGrrolcyTest. MachineNa
Uown-Sysmon TimeCreated /Date(17P6780#528236)/ _id WWcRREMFλaHerBvl./5RI _ignonId - _idaex sumben-rew _acore 3 - _LeviooersName

Message File created:: RuleName: - UtcTime· 2026-02-10 06:145.662 ProversGuid: [redacted] ProcessGuid: powershell.exe
Image: C:\Windows\System3a\local\Temp\__PSScriptPolicyTest_08396Pwo.my2.ox3 CreationUtcIime: 2026-02-10 18:45:55.855 Usser: PrSSipopa
Howp-Sysmon TimeCreated /Date(17P67040826273)/ _id W06RR6MFλ3Herxop.2REI _ignored - _index symmer-rew _acore 3 [redacted]

Message File created:: RuleName: - UtcTime· 2026-02-10 06:145.606 ProwersGuid: [redacted] ProcessGuid: Powershell.exe
Image: C:\Windows\SysDet3A\local\Temp\__PSScriptPolicyTest_mo#8o).ny3.Wa.10 CreationUcTime: 2026-02-00 10:40:55:21.636 Ueser: MachineNa
Hown-Sysmon TimeCreated /Date(17P66780638238)/ _id W06RR2MEZaAesBvl./EEl _ignon8d - _index syumon-rew _acore 3 [redacted]

Message File created:: RuleName: - UtcTime· 2026-02-10 16:345.648 ProwersGuid: [redacted] ProcessGuid: Powershell.exe
Image: C:\Windows\System32\local\Temp\__PSScriptPolicyTest_30896Jror.my2.ps5 CreationUtcTime: 2026-02-10 16:37:36.738 Uuser: PrsSippa
Hown-Sysmon TimeCreated /Date(17P67048828738)/ _id WWcRR2MEλaAerBvl.2HME _ignonId - _index syumon-rew _acore 3 [redacted]

Message File created:: RuleName: - UtcTime· 2026-02-10 06:305.615 ProwersGuid: [redacted] ProcessGuid: Powershell.exe
Image: C:\Windows\System3a\local\Temp\__PSScriptPolicyTest_94886Poo.my3.ox3 CreationUtcTime: 2026-02-10 06:53:26 465 Ueser: MachineNa
down-Sysmon TimeCreated /Date(17P66784636037)/ _id WAcRR2MFλaHorBvl.2ERE _ignonId - _index symnen-rew _acore 3 [redacted]

Message File created:: RuleName: - UtcTime· 2026-02-00 17:345.437 ProversGuid: [redacted] ProcessGuid: powershell.exe
Image: C:\Windows\SysDet3a\local\Temp\__PSScriptPolicyTest_90896Poo.my3.ex3 CreationUtcTime: 2026-02-00 13:33:26 859 Ueser: MachineNa
down-Sysmon TimeCreated /Date(77P66720228253)/ _id WAcRR5MFλaWerBvl./SEI _ignored - _index symmen-rew _acore 3 [redacted]

Message File created:: RuleName: - UtcTime: 2026-02-10 15:545:074 ProwersGuid: [redacted] ProcessGuid: powershell.exe
Image: C:\Windows\System3a\local\Temp\__PSScriptPolicyTest_waoaShor.wp1.ex3 CreationUtcTime: 2026-02-00 13:33:36 056 Ueser: MachineNa
Hown-Sysmon TimeCreated /Date((7P65770236253)/ _id W0cRR6MF3aWerBvl./SEl _ignored - _index symmen-raw _acore 3 [redacted]
```

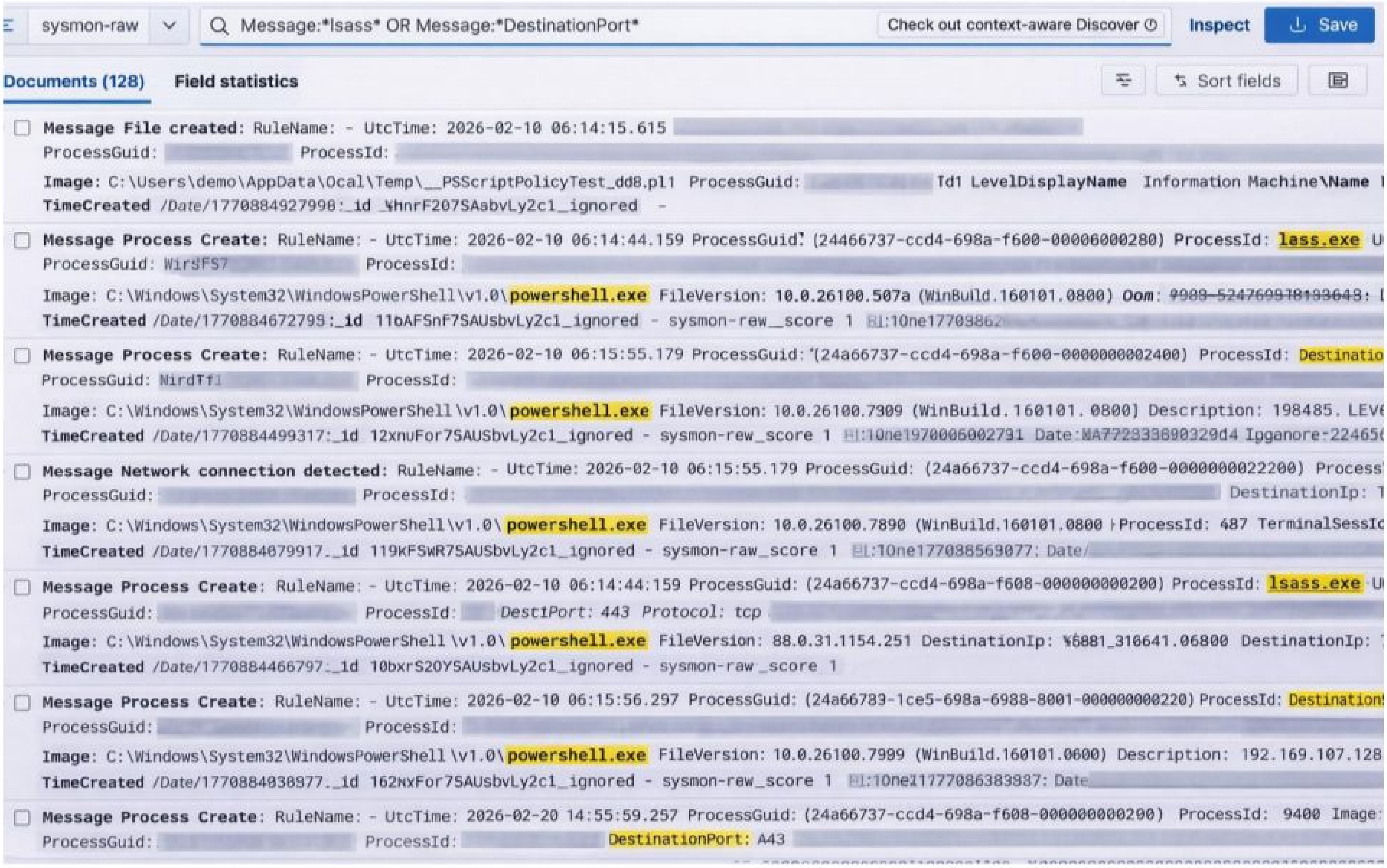
6. LSASS with Network Port Correlation

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
Message:*lsass* OR Message:*DestinationPort*
```

```
□ Message File created: RuleName: - UtcTime: 2026-02-10 06:14:15.615 [redacted]
  ProcessGuid: [redacted] ProcessId: [redacted]
  Image: C:\Users\demo\AppData\Ocal\Temp\__PSScriptPolicyTest_dd8.pl1 ProcessGuid: [redacted] Id1 LevelDisplayName Information Machine\Name
  TimeCreated /Date/1770884927998:_id_%hnrF207SAabvLy2c1_ignored  -

□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:14:44.159 ProcessGuid: (24466737-ccd4-698a-f600-00006000280) ProcessId: lass.exe U
  ProcessGuid: [redacted] ProcessId: [redacted]
  Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0.26100.507a (WinBuild.160101.0800) Oom: ~~9988-5247699181933648~~:
  TimeCreated /Date/1770884672795:_id 11oAFSnF7SAUSbvLy2c1_ignored - sysmon-rew__score 1 [redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:15:55.179 ProcessGuid:'(24a66737-ccd4-698a-f600-0000000002400) ProcessId: Destinatio
  ProcessGuid: [redacted] ProcessId: [redacted]
  Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0.26100.7909 (WinBuild.160101. 0800] Description: 198485. LEV
  TimeCreated /Date/1770884499317:_id 12xnuFor7SAUSbvLy2c1_ignored - sysmon-rew_score 1 [redacted]

□ Message Network connection detected: RuleName: - UtcTime: 2026-02-10 06:15:55.179 ProcessGuid: (24a66737-ccd4-698a-f600-0000000022200) Process
  ProcessGuid: [redacted] ProcessId: [redacted] DestinationIp: 
  Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe FileVersion: 10.0.26100.7890 (WinBuild.160101.0800 ⟩ProcessId: 487 TerminalSessIc
  TimeCreated /Date/1770884079917._id 119KFSWR7SAUSbvLy2c1_ignored - sysmon-raw_score 1 [redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:14:44:159 ProcessGuid: (24a66737-ccd4-698a-f608-000000000200) ProcessId: lsass.exe U
  ProcessGuid: [redacted] ProcessId: [redacted] DestiPort: 443 Protocol: tcp [redacted]
  Image: C:\Windows\System32\WindowsPowerShell \v1.0\ powershell.exe FileVersion: 88.0.31.1154.251 DestinationIp: ¥6881_310641.06800 DestinationIp:
  TimeCreated /Date/1770884466797._id 10bxrS20YSAUSbvLy2c1_ignored - sysmon-raw _score 1

□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:15:56.257 ProcessGuid: (24a66783-1ce5-698a-6988-8001-000000000220) ProcessId: Destination
  ProcessGuid: [redacted] ProcessId: [redacted]
  Image: C:\Windows\System32\WindowsPowerShell \v1.0\powershell.exe FileVersion: 10.0.26100.7999 (WinBuild.160101.0600) Description: 192.169.107.128
  TimeCreated /Date/1770884038977._id 162NxFor7SAUSbvLy2c1_ignored - sysmon-rew_score 1 [redacted]

□ Message Process Create: RuleName: - UtcTime: 2026-02-20 14:55:59.257 ProcessGuid: (24a66737-ccd4-698a-f608-000000000290) ProcessId: 9400 Image:
  ProcessGuid: [redacted] ProcessId: [redacted] DestinationPort: A43 [redacted]
```

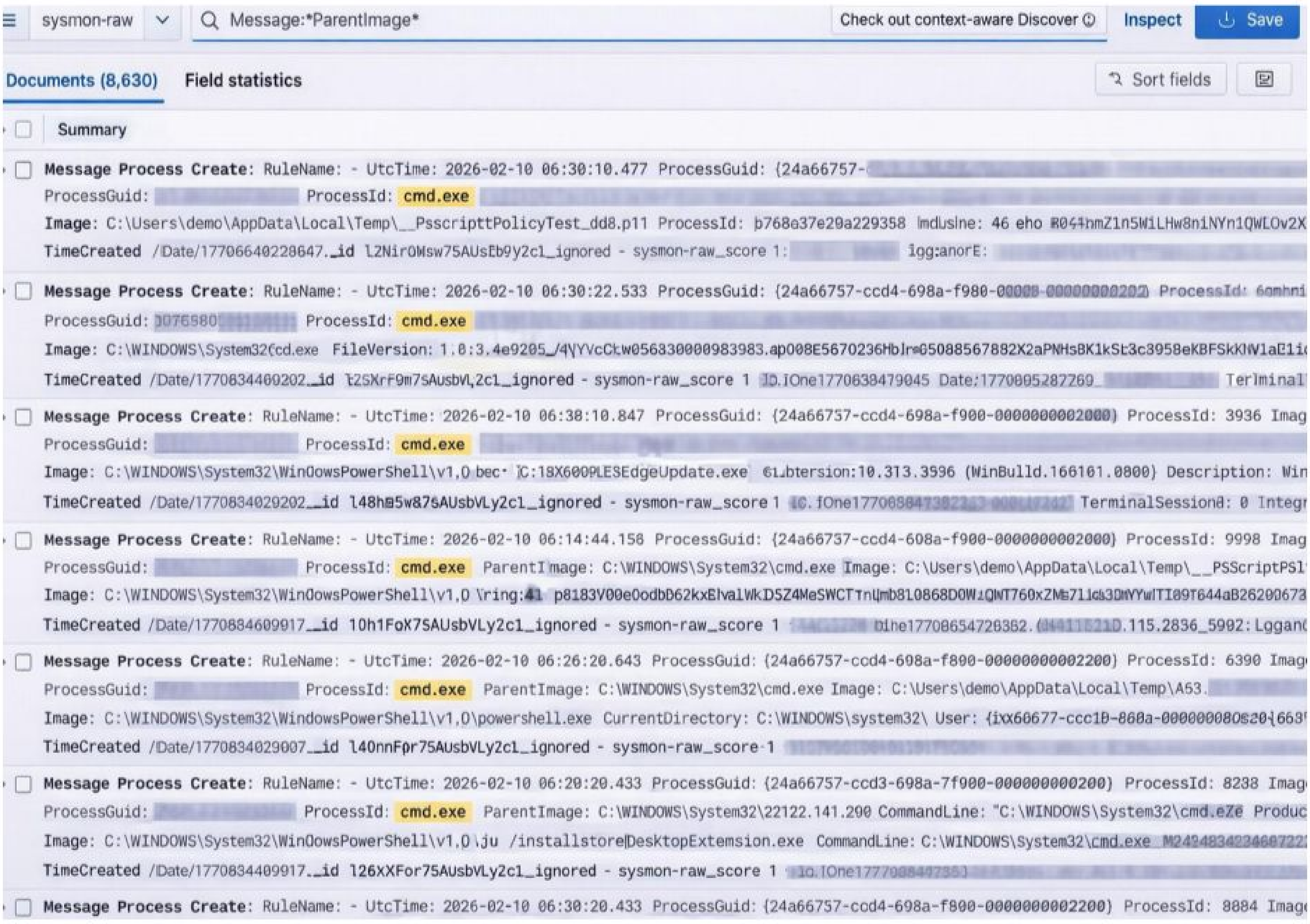
7. RunOnce Registry Persistence Detection

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



Message:*ParentImage*

Documents (8,630)

□ Summary

```
□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:30:10.477 ProcessGuid: {24a66757-[redacted]
  ProcessGuid: [redacted] ProcessId: cmd.exe [redacted]
  Image: C:\Users\demo\AppData\Local\Temp\__PsscripttPolicyTest_dd8.p11 ProcessId: b768e37e20a229358 lmdusine: 46 eho R04+hmZ1n5WiLHw8n1NYn1QWLOv2X
  TimeCreated /Date/17706640228647._id l2NirOMsw75AUsEb9y2cl_ignored - sysmon-raw_score 1: [redacted] igg:anorE: [redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:30:22.533 ProcessGuid: {24a66757-ccd4-698a-f980-[redacted] ProcessId: [redacted]
  ProcessGuid: [redacted] ProcessId: cmd.exe [redacted]
  Image: C:\WINDOWS\System32(cd.exe  FileVersion: 1.0:3.4e9205_/4\YVcCkw056830000983983.ap008E5670236Hblr=05088567882X2aPNHsBK1kSt3c3958eKBFSkKNV1aE1i
  TimeCreated /Date/1770834400202._id t2SXrF9m7sAusbVL2cl_ignored - sysmon-raw_score 1 [redacted] Date:1770805287269_[redacted] Terlminal
□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:38:10.847 ProcessGuid: {24a66757-ccd4-698a-f900-000000002000) ProcessId: 3936 Imag
  ProcessGuid: [redacted] ProcessId: cmd.exe [redacted]
  Image: C:\WINDOWS\System32\WinOowsPowerShell\v1,0 bec· ]C:18X600PLESEdgeUpdate.exe  61ubtersion:10.313.3596 (WinBulld.166161.0800) Description: Win
  TimeCreated /Date/1770834029202._id 148h85w87sAUsbVLy2cl_ignored - sysmon-raw_score 1 [redacted] TerminalSession8: 0 Integr
□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:14:44.158 ProcessGuid: {24a66757-ccd4-608a-f900-000000002000) ProcessId: 9998 Imag
  ProcessGuid: [redacted] ProcessId: cmd.exe  ParentImage: C:\WINDOWS\System32\cmd.exe Image: C:\Users\demo\AppData\Local\Temp\__PSScriptPS1
  Image: C:\WINDOWS\System32\WinOowsPowerShell\v1,0 \ring:41  p8183V00e0odbD62kxElvalWkD5Z4MeSWCTтnЏmb810868D0W₁QWT760xZMs71ıc&3DMYYwlTI89T644aB26200673
  TimeCreated /Date/1770884609917._id 10h1FoX7SAUsbVLy2cl_ignored - sysmon-raw_score 1 [redacted] b1ne17708654726362.[redacted].115.2836_5992:Lgganc
□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:26:20.643 ProcessGuid: {24a66757-ccd4-698a-f800-00000000002200) ProcessId: 6390 Imag
  ProcessGuid: [redacted] ProcessId: cmd.exe  ParentImage: C:\WINDOWS\System32\cmd.exe Image: C:\Users\demo\AppData\Local\Temp\A53.[redacted]
  Image: C:\WINDOWS\System32\WindowsPowerShell\v1,0\powershell.exe CurrentDirectory: C:\WINDOWS\system32\ User: {ixx60677-ccc1D-860a-00000008O820{663
  TimeCreated /Date/1770834029007._id l40nnFpr75AUsbVLy2cl_ignored - sysmon-raw_score 1 [redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:20:20.433 ProcessGuid: {24a66757-ccd3-698a-7f900-000000000200) ProcessId: 8238 Imag
  ProcessGuid: [redacted] ProcessId: cmd.exe  ParentImage: C:\WINDOWS\System32\22122.141.290 CommandLine: "C:\WINDOWS\System32\cmd.eZe Produc
  Image: C:\WINDOWS\System32\WinOowsPowerShell\v1,0 \ju /installstore|DesktopExtemsion.exe  CommandLine: C:\WINDOWS\System32\cmd.exe M242483422466722
  TimeCreated /Date/1770834409917._id l26XXFor75AUsbVLy2cl_ignored - sysmon-raw_score 1 [redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:30:20.433 ProcessGuid: {24a66757-ccd4-698a-f800-0000000002200) ProcessId: 8884 Imag
```

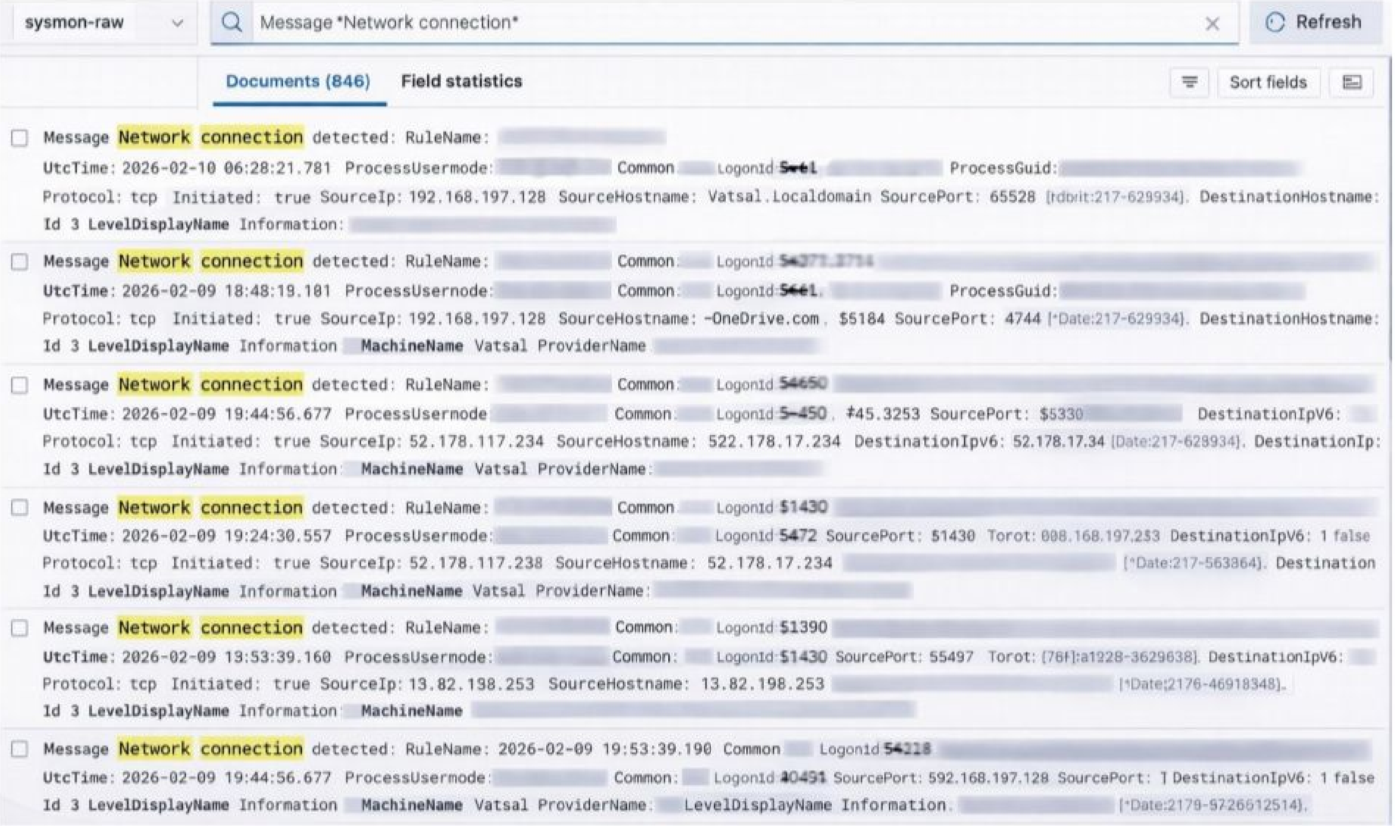
8. Outbound Network Communication Analysis

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
□ Message Network connection detected: RuleName: [redacted]
  UtcTime: 2026-02-10 06:28:21.781 ProcessUsermode: [redacted] Common [redacted] LogonId [redacted] [redacted] ProcessGuid: [redacted]
  Protocol: tcp Initiated: true SourceIp: 192.168.197.128 SourceHostname: Vatsal.Localdomain SourcePort: 65528 [tdbit:217-629934]. DestinationHostname:
  Id 3 LevelDisplayName Information: [redacted]

□ Message Network connection detected: RuleName: [redacted] Common: [redacted] LogonId [redacted] [redacted]
  UtcTime: 2026-02-09 18:48:19.101 ProcessUsernode: [redacted] Common: [redacted] LogonId [redacted]. [redacted] ProcessGuid: [redacted]
  Protocol: tcp Initiated: true SourceIp: 192.168.197.128 SourceHostname: -OneDrive.com . $5184 SourcePort: 4744 [*Date:217-629934]. DestinationHostname:
  Id 3 LevelDisplayName Information [redacted] MachineName Vatsal ProviderName [redacted]

□ Message Network connection detected: RuleName: [redacted] Common: [redacted] LogonId [redacted] [redacted]
  UtcTime: 2026-02-09 19:44:56.677 ProcessUsermode [redacted] Common: [redacted] LogonId [redacted] . ‡45.3253 SourcePort: $5330 [redacted] DestinationIpV6: [redacted]
  Protocol: tcp Initiated: true SourceIp: 52.178.117.234 SourceHostname: 522.178.17.234 DestinationIpv6: 52.178.17.34 [Date:217-628934]. DestinationIp:
  Id 3 LevelDisplayName Information: [redacted] MachineName Vatsal ProviderName: [redacted]

□ Message Network connection detected: RuleName: [redacted] Common [redacted] LogonId $1430 [redacted]
  UtcTime: 2026-02-09 19:24:30.557 ProcessUsermode: [redacted] Common: [redacted] LogonId 5472 SourcePort: $1430 Torot: 008.168.197.253 DestinationIpV6: 1 false
  Protocol: tcp Initiated: true SourceIp: 52.178.117.238 SourceHostname: 52.178.17.234 [redacted] [*Date:217-563864]. Destination
  Id 3 LevelDisplayName Information [redacted] MachineName Vatsal ProviderName: [redacted]

□ Message Network connection detected: RuleName: [redacted] Common: [redacted] LogonId $1390 [redacted]
  UtcTime: 2026-02-09 13:53:39.160 ProcessUsernode: [redacted] Common: [redacted] LogonId $1430 SourcePort: 55497 Torot: [76f]:a1928-3629638]. DestinationIpV6: [redacted]
  Protocol: tcp Initiated: true SourceIp: 13.82.198.253 SourceHostname: 13.82.198.253 [redacted] [*Date;2176-46918348].
  Id 3 LevelDisplayName Information [redacted] MachineName [redacted]

□ Message Network connection detected: RuleName: 2026-02-09 19:53:39.190 Common [redacted] LogonId [redacted] [redacted]
  UtcTime: 2026-02-09 19:44:56.677 ProcessUsermode: [redacted] Common: [redacted] LogonId [redacted] SourcePort: 592.168.197.128 SourcePort: 1 DestinationIpV6: 1 false
  Id 3 LevelDisplayName Information [redacted] MachineName Vatsal ProviderName: [redacted] LevelDisplayName Information. [redacted] [*Date:2179-9726612514].
```

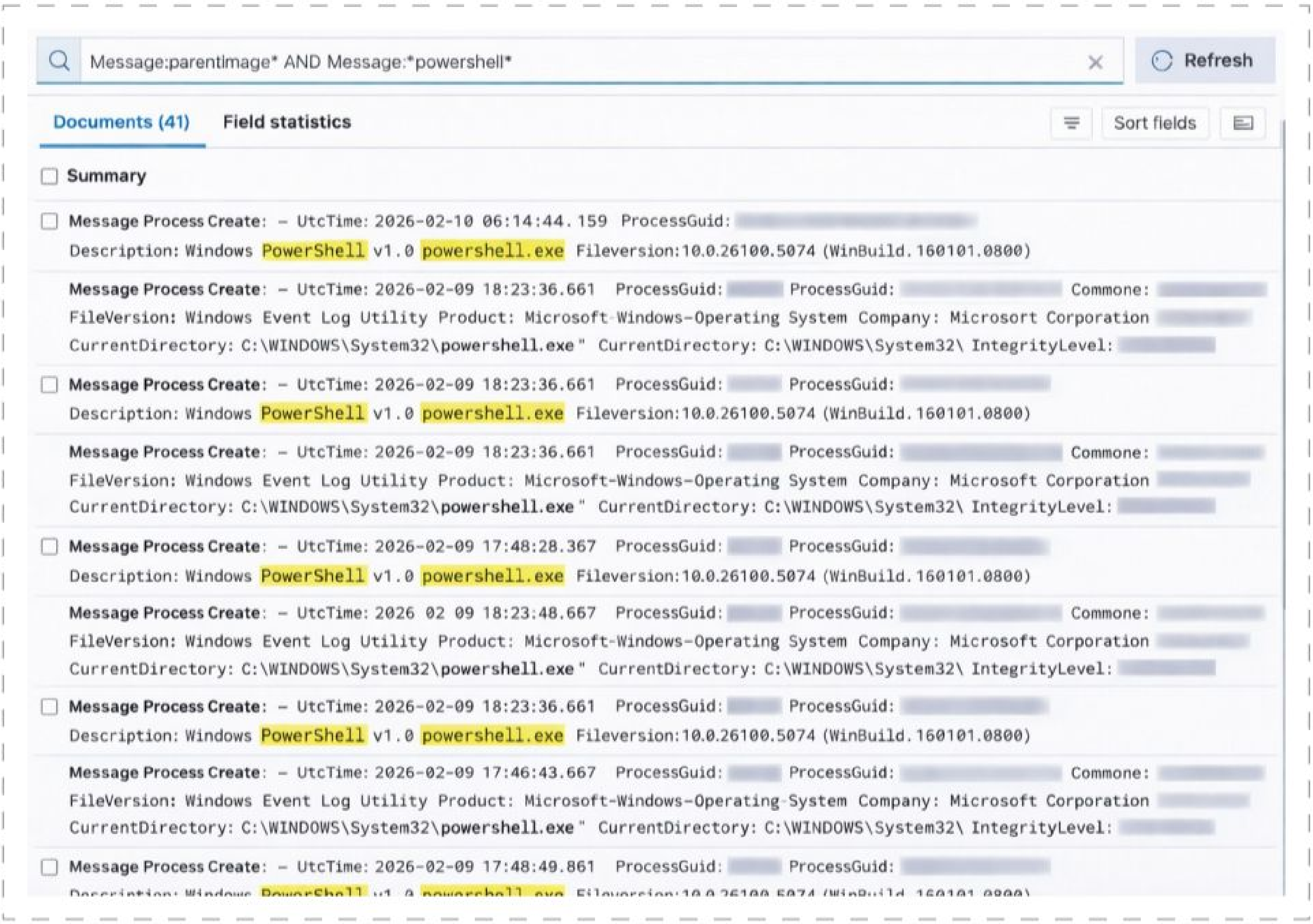
9. Repeated ParentImage PowerShell Execution

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
Message:parentimage* AND Message:*powershell*
```

```
□ Message Process Create: – UtcTime: 2026-02-10 06:14:44. 159  ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild. 160101.0800)
  Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating System Company: Microsort Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
□ Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild. 160101.0800)
  Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating System Company: Microsoft Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
□ Message Process Create: – UtcTime: 2026-02-09 17:48:28.367  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild. 160101.0800)
  Message Process Create: – UtcTime: 2026 02 09 18:23:48.667  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating System Company: Microsoft Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
□ Message Process Create: – UtcTime: 2026-02-09 18:23:36.661  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild. 160101.0800)
  Message Process Create: – UtcTime: 2026-02-09 17:46:43.667  ProcessGuid: [redacted] ProcessGuid: [redacted] Commone: [redacted]
  FileVersion: Windows Event Log Utility Product: Microsoft-Windows-Operating System Company: Microsoft Corporation [redacted]
  CurrentDirectory: C:\WINDOWS\System32\powershell.exe" CurrentDirectory: C:\WINDOWS\System32\ IntegrityLevel: [redacted]
□ Message Process Create: – UtcTime: 2026-02-09 17:48:49.861  ProcessGuid: [redacted] ProcessGuid: [redacted]
  Description: Windows PowerShell v1.0 powershell.exe Fileversion:10.0.26100.5074 (WinBuild. 160101.0800)
```

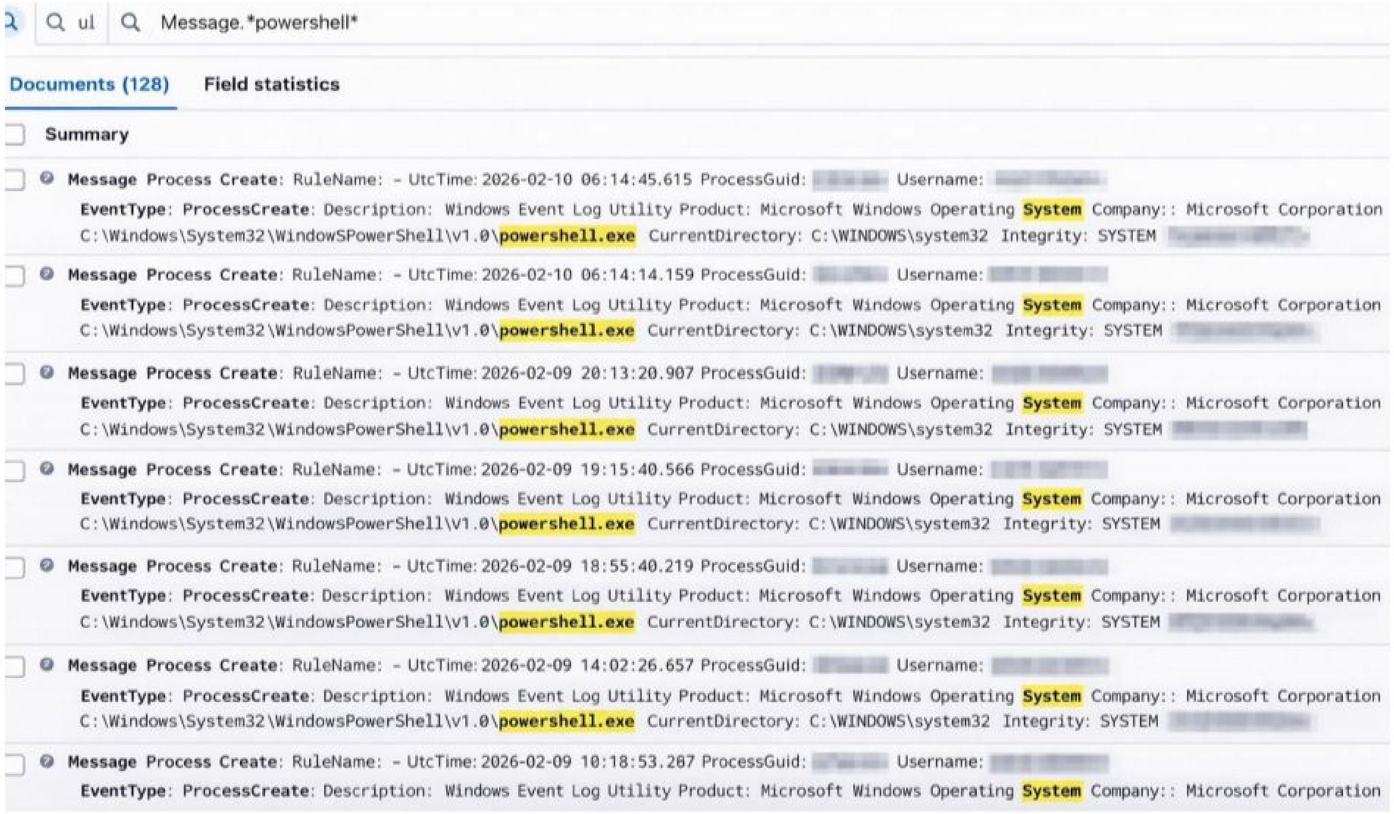
10. SYSTEM-Level PowerShell Execution

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



Message.*powershell*

```
Message Process Create: RuleName: - UtcTime: 2026-02-10 06:14:45.615 ProcessGuid: [redacted] Username: [redacted]
  EventType: ProcessCreate: Description: Windows Event Log Utility Product: Microsoft Windows Operating System Company:: Microsoft Corporation
  C:\Windows\System32\WindowSPowerShell\v1.0\powershell.exe CurrentDirectory: C:\WINDOWS\system32 Integrity: SYSTEM [redacted]
Message Process Create: RuleName: - UtcTime: 2026-02-10 06:14:14.159 ProcessGuid: [redacted] Username: [redacted]
  EventType: ProcessCreate: Description: Windows Event Log Utility Product: Microsoft Windows Operating System Company:: Microsoft Corporation
  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe CurrentDirectory: C:\WINDOWS\system32 Integrity: SYSTEM [redacted]
Message Process Create: RuleName: - UtcTime: 2026-02-09 20:13:20.907 ProcessGuid: [redacted] Username: [redacted]
  EventType: ProcessCreate: Description: Windows Event Log Utility Product: Microsoft Windows Operating System Company:: Microsoft Corporation
  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe CurrentDirectory: C:\WINDOWS\system32 Integrity: SYSTEM [redacted]
Message Process Create: RuleName: - UtcTime: 2026-02-09 19:15:40.566 ProcessGuid: [redacted] Username: [redacted]
  EventType: ProcessCreate: Description: Windows Event Log Utility Product: Microsoft Windows Operating System Company:: Microsoft Corporation
  C:\Windows\System32\WindowsPowerShell\V1.0\powershell.exe CurrentDirectory: C:\WINDOWS\system32 Integrity: SYSTEM [redacted]
Message Process Create: RuleName: - UtcTime: 2026-02-09 18:55:40.219 ProcessGuid: [redacted] Username: [redacted]
  EventType: ProcessCreate: Description: Windows Event Log Utility Product: Microsoft Windows Operating System Company:: Microsoft Corporation
  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe CurrentDirectory: C:\WINDOWS\system32 Integrity: SYSTEM [redacted]
Message Process Create: RuleName: - UtcTime: 2026-02-09 14:02:26.657 ProcessGuid: [redacted] Username: [redacted]
  EventType: ProcessCreate: Description: Windows Event Log Utility Product: Microsoft Windows Operating System Company:: Microsoft Corporation
  C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe CurrentDirectory: C:\WINDOWS\system32 Integrity: SYSTEM [redacted]
Message Process Create: RuleName: - UtcTime: 2026-02-09 10:18:53.287 ProcessGuid: [redacted] Username: [redacted]
  EventType: ProcessCreate: Description: Windows Event Log Utility Product: Microsoft Windows Operating System Company:: Microsoft Corporation
```

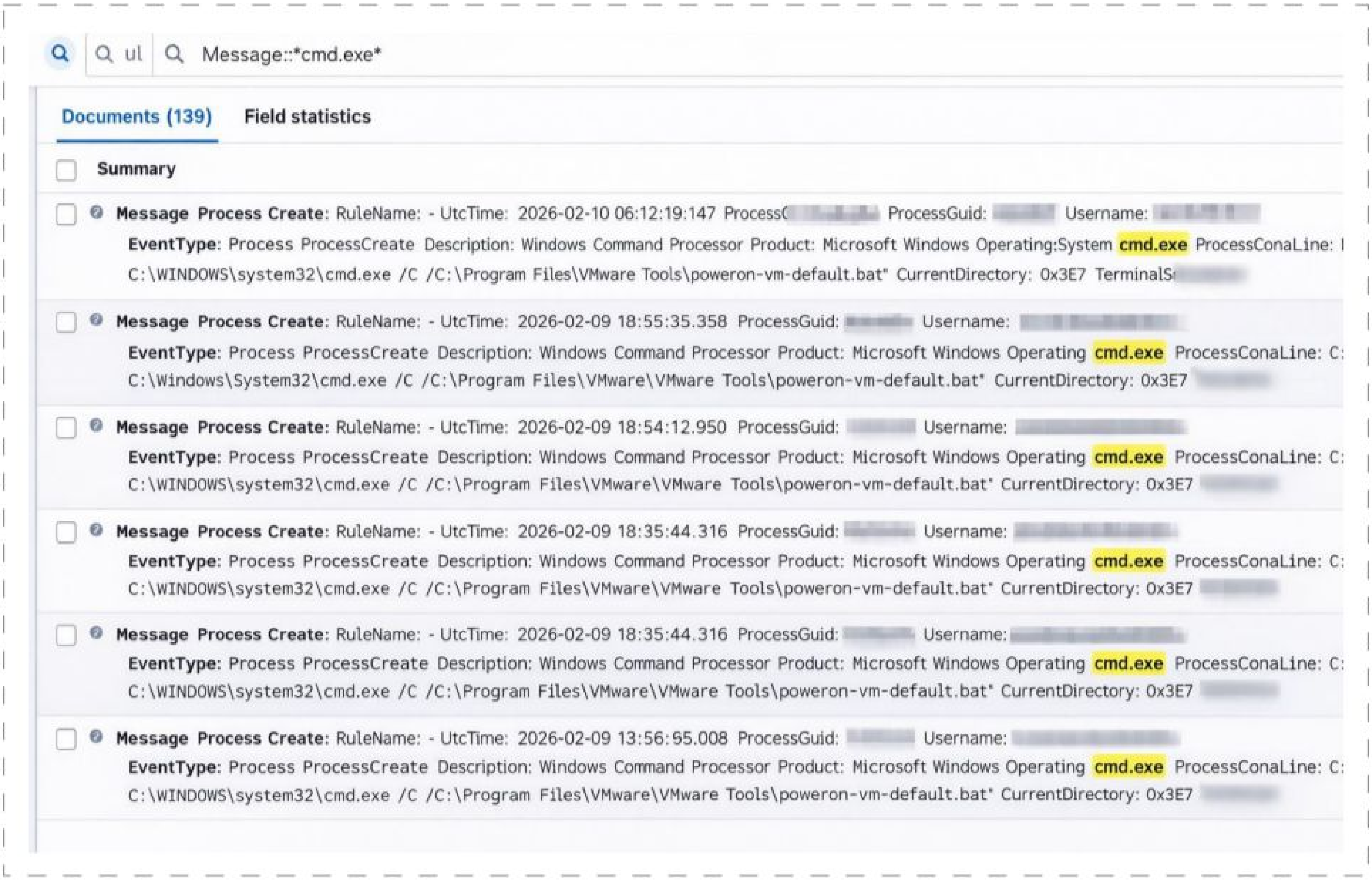
11. Command Prompt Execution Pattern Analysis

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
Message::*cmd.exe*

□ Message Process Create: RuleName: - UtcTime: 2026-02-10 06:12:19:147 ProcessC[redacted] ProcessGuid: [redacted] Username: [redacted]
  EventType: Process ProcessCreate Description: Windows Command Processor Product: Microsoft Windows Operating:System cmd.exe ProcessConaLine: I
  C:\WINDOWS\system32\cmd.exe /C /C:\Program Files\VMware Tools\poweron-vm-default.bat" CurrentDirectory: 0x3E7 TerminalS[redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-09 18:55:35.358 ProcessGuid: [redacted] Username: [redacted]
  EventType: Process ProcessCreate Description: Windows Command Processor Product: Microsoft Windows Operating cmd.exe ProcessConaLine: C:
  C:\Windows\System32\cmd.exe /C /C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat" CurrentDirectory: 0x3E7 [redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-09 18:54:12.950 ProcessGuid: [redacted] Username: [redacted]
  EventType: Process ProcessCreate Description: Windows Command Processor Product: Microsoft Windows Operating cmd.exe ProcessConaLine: C:
  C:\WINDOWS\system32\cmd.exe /C /C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat" CurrentDirectory: 0x3E7 [redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-09 18:35:44.316 ProcessGuid: [redacted] Username: [redacted]
  EventType: Process ProcessCreate Description: Windows Command Processor Product: Microsoft Windows Operating cmd.exe ProcessConaLine: C:
  C:\WINDOWS\system32\cmd.exe /C /C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat" CurrentDirectory: 0x3E7 [redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-09 18:35:44.316 ProcessGuid: [redacted] Username: [redacted]
  EventType: Process ProcessCreate Description: Windows Command Processor Product: Microsoft Windows Operating cmd.exe ProcessConaLine: C:
  C:\WINDOWS\system32\cmd.exe /C /C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat" CurrentDirectory: 0x3E7 [redacted]
□ Message Process Create: RuleName: - UtcTime: 2026-02-09 13:56:95.008 ProcessGuid: [redacted] Username: [redacted]
  EventType: Process ProcessCreate Description: Windows Command Processor Product: Microsoft Windows Operating cmd.exe ProcessConaLine: C:
  C:\WINDOWS\system32\cmd.exe /C /C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat" CurrentDirectory: 0x3E7 [redacted]
```

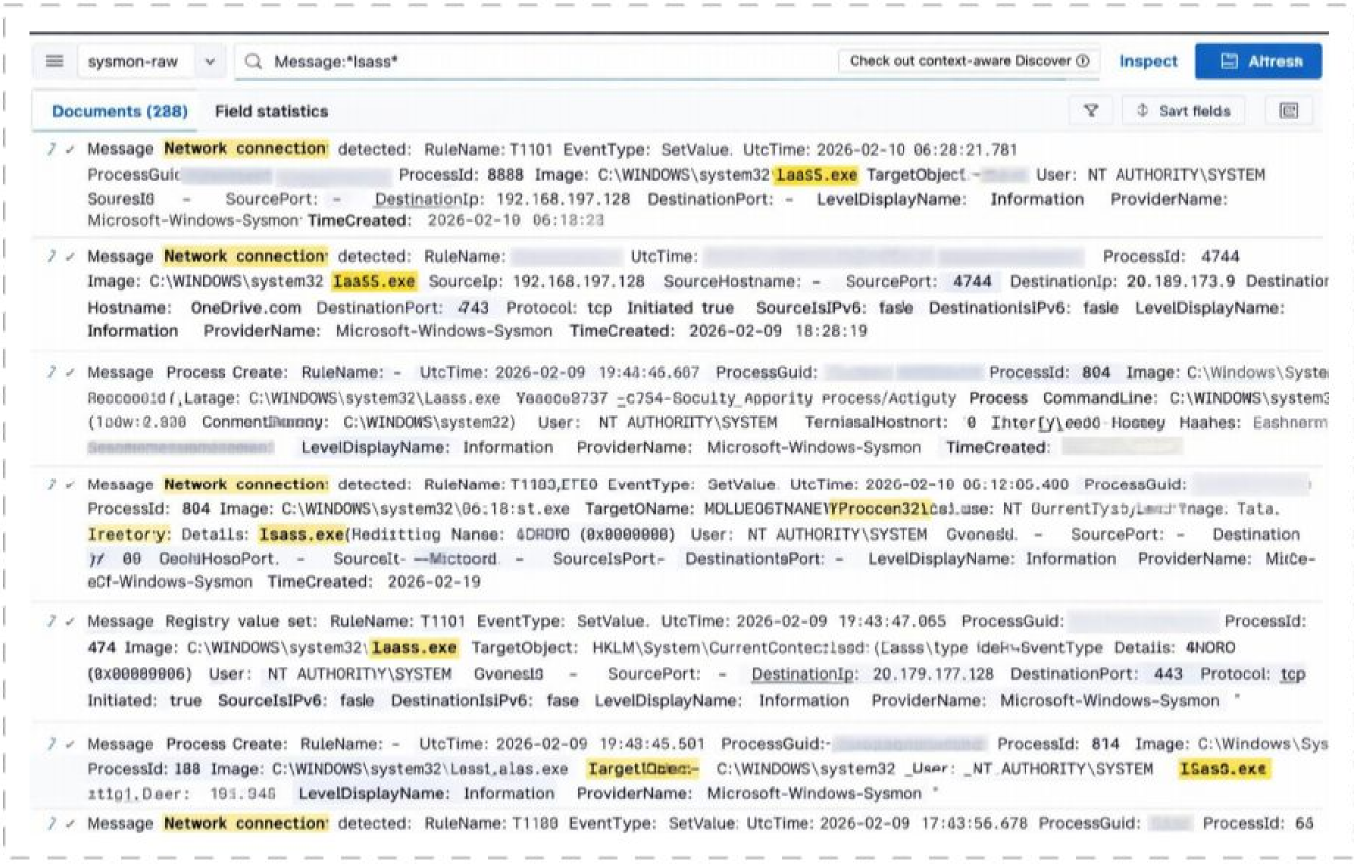
12. Credential Access Pattern (LSASS Detailed View)

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



Message:*lsass*

```
Message Network connection detected: RuleName: T1101 EventType: SetValue. UtcTime: 2026-02-10 06:28:21.781
ProcessGuic [redacted] ProcessId: 8888 Image: C:\WINDOWS\system32 LaaSS.exe TargetObject - [redacted] User: NT AUTHORITY\SYSTEM
SouresIG - SourcePort: - DestinationIp: 192.168.197.128 DestinationPort: - LevelDisplayName: Information ProviderName:
Microsoft-Windows-Sysmon TimeCreated: 2026-02-10 06:18:23

Message Network connection detected: RuleName: [redacted] UtcTime: [redacted] ProcessId: 4744
Image: C:\WINDOWS\system32 IaaSS.exe SourceIp: 192.168.197.128 SourceHostname: - SourcePort: 4744 DestinationIp: 20.189.173.9 Destinatior
Hostname: OneDrive.com DestinationPort: 443 Protocol: tcp Initiated true SourceIsIPv6: fasle DestinationIsIPv6: fasle LevelDisplayName:
Information ProviderName: Microsoft-Windows-Sysmon TimeCreated: 2026-02-09 18:28:19

Message Process Create: RuleName: - UtcTime: 2026-02-09 19:44:46.607 ProcessGuid: [redacted] ProcessId: 804 Image: C:\Windows\Syste
Reccoo0id(,Latage: C:\WINDOWS\system32\Laass.exe Yeaece8737 -c754-Soculty_Appority process/Actiguty Process CommandLine: C:\WINDOWS\system3
(1odw:2.800 ConmentIReeny: C:\WINDOWS\system22) User: NT AUTHORIITY\SYSTEM TerniasalHostnort: 0 Ihter[y\eedo Hoseey Haahes: Eashnerm
[redacted] LevelDisplayName: Information ProviderName: Microsoft-Windows-Sysmon TimeCreated: [redacted]

Message Network connection detected: RuleName: T1103,ETEO EventType: SetValue UtcTime: 2026-02-10 06:12:05.400 ProcessGuid: [redacted]
ProcessId: 804 Image: C:\WINDOWS\system32\06:18:st.exe TargetOName: MDLUEO6TNANEWProccen321cel.use: NT OurrentTysb/Lmd Tnage: Tata.
Ireetory: Details: Isass.exe(Hedittiog Nanee: 4DROYO (0x0000000) User: NT AUTHORITY\SYSTEM Gvenesd. - SourcePort: - Destination
)/ 00 OeolliHosoPort. - SourceIt- —Mictoord - SourceIsPort- DestinationtsPort: - LevelDisplayName: Information ProviderName: MiCe-
eCf-Windows-Sysmon TimeCreated: 2026-02-19

Message Registry value set: RuleName: T1101 EventType: SetValue. UtcTime: 2026-02-09 19:43:47.065 ProcessGuid: [redacted] ProcessId:
474 Image: C:\WINDOWS\system32\Laass.exe TargetObject: HKLM\System\CurrentContectlsod:(Lasss\type ideH-SventType Details: 4NORO
(0x00009006) User: NT AUTHORITY\SYSTEM GvenesIG - SourcePort: - DestinationIp: 20.179.177.128 DestinationPort: 443 Protocol: tcp
Initiated: true SourceIsIPv6: fasle DestinationIsiPv6: fase LevelDisplayName: Information ProviderName: Microsoft-Windows-Sysmon "

Message Process Create: RuleName: - UtcTime: 2026-02-09 19:43:45.501 ProcessGuid:-[redacted] ProcessId: 814 Image: C:\Windows\Sys
ProcessId: 188 Image: C:\WINDOWS\system32\Lesst,alas.exe TargetIOeec:- C:\WINDOWS\system32 _User: _NT AUTHORITY\SYSTEM ISasS.exe
ztig1,Deer: 195.946 LevelDisplayName: Information ProviderName: Microsoft-Windows-Sysmon "

Message Network connection detected: RuleName: T1180 EventType: SetValue: UtcTime: 2026-02-09 17:43:56.678 ProcessGuid: [redacted] ProcessId: 66
```

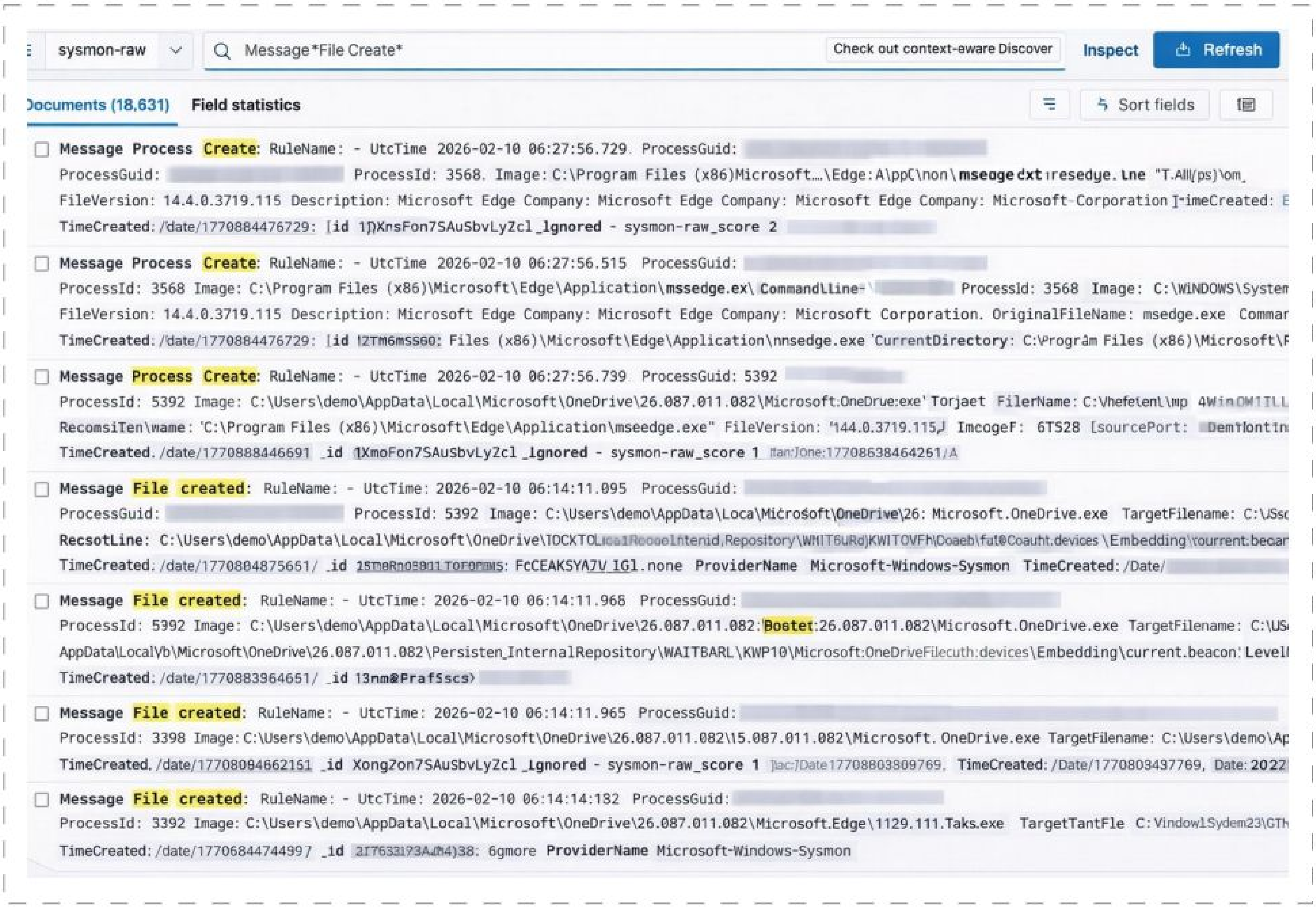
13. Suspicious File Creation & Payload Staging

Detection Objective: Identify suspicious behavior based on Sysmon event telemetry.

Technical Explanation: Analysis performed using Elastic KQL queries against sysmon-raw index focusing on Event ID 1 (Process Create), Event ID 3 (Network Connection), Event ID 11 (File Create), and Event ID 13 (Registry Events).

Behavioral Risk Assessment: This behavior contributes to execution, persistence, credential access, or command-and-control phases of an attack lifecycle.

Analyst Interpretation: Individual events may appear benign; however, when correlated within the same timeframe, they strongly indicate pre-ransomware staging activity.



```
□ Message Process Create: RuleName: - UtcTime 2026-02-10 06:27:56.729. ProcessGuid: [redacted]
  ProcessGuid: [redacted] ProcessId: 3568. Image: C:\Program Files (x86)Microsoft…\Edge:A\ppC\non\mseoge dxt ıresedye. lne "T.All/ps)\om,
  FileVersion: 14.4.0.3719.115 Description: Microsoft Edge Company: Microsoft Edge Company: Microsoft Edge Company: Microsoft-Corporation I-imeCreated: E
  TimeCreated: /date/1770884476729: [id 1ŊXnsFon7SAuSbvLyZcl _lgnored - sysmon-raw_score 2 [redacted]

□ Message Process Create: RuleName: - UtcTime 2026-02-10 06:27:56.515 ProcessGuid: [redacted]
  ProcessId: 3568 Image: C:\Program Files (x86)\Microsoft\Edge\Application\mssedge.ex\ CommandLline-\ [redacted] ProcessId: 3568 Image: C:\WiNDOWS\System
  FileVersion: 14.4.0.3719.115 Description: Microsoft Edge Company: Microsoft Edge Company: Microsoft Corporation. OriginalFileName: msedge.exe Commar
  TimeCreated: /date/1770884476729: [id !2TM6mSS60: Files (x86)\Microsoft\Edge\Application\nnsedge.exe 'CurrentDirectory: C:\Prográm Files (x86)\Microsoft\F

□ Message Process Create: RuleName: - UtcTime 2026-02-10 06:27:56.739 ProcessGuid: 5392 [redacted]
  ProcessId: 5392 Image: C:\Users\demo\AppData\Local\Microsoft\OneDrive\26.087.011.082\Microsoft:OneDrue:exe' Torjaet FilerName: C:\hefeLenL\mp 4WinOM1TLL
  RecomsiTen\wame: 'C:\Program Files (x86)\Microsoft\Edge\Application\mseedge.exe" FileVersion: '144.0.3719.115,J ImcogeF: 6TS28 [sourcePort: Dem†lontin
  TimeCreated. /date/1770888446691 _id 1XmoFon7SAuSbvLyZcl _lgnored - sysmon-raw_score 1 ltan:lOne:17708638464261/A

□ Message File created: RuleName: - UtcTime: 2026-02-10 06:14:11.095 ProcessGuid: [redacted]
  ProcessGuid: [redacted] ProcessId: 5392 Image: C:\Users\demo\AppData\Loca\Mićrosoft\OneDrive\26: Microsoft.OneDrive.exe TargetFilename: C:\USsc
  RecsotLine: C:\Users\demo\AppData\Local\Microsoft\OneDrive\IOCKTOLica1Rooeelntenid,Repository\WMIT6uRd)KWITOVFh\Coaeb\fut@Coauht.devices\Embedding\current.becar
  TimeCreated. /date/1770804875661/ _id 15TmoRno8801TOrofmms: FcCEAKSYA7V_IGl.none ProviderName Microsoft-Windows-Sysmon TimeCreated: /Date/ [redacted]

□ Message File created: RuleName: - UtcTime: 2026-02-10 06:14:11.968 ProcessGuid: [redacted]
  ProcessId: 5392 Image: C:\Users\demo\AppData\Local\Microsoft\OneDrive\26.087.011.082:Bostet:26.087.011.082\Microsoft.OneDrive.exe TargetFilename: C:\US
  AppData\LocalVb\Microsoft\OneDrive\26.087.011.082\Persisten_InternalRepository\WAITBARL\KWP10\Microsoft:OneDriveFilecuth:devices\Embedding\current.beacon: Levell
  TimeCreated: /date/1770883964651/ _id 13nm@PrafSscs› [redacted]

□ Message File created: RuleName: - UtcTime: 2026-02-10 06:14:11.965 ProcessGuid: [redacted]
  ProcessId: 3398 Image: C:\Users\demo\AppData\Local\Microsoft\OneDrive\26.087.011.082\15.087.011.082\Microsoft. OneDrive.exe TargetFilename: C:\Users\demo\Ap
  TimeCreated. /date/17708084662151 _id XongZon7SAuSbvLyZcl _ignored - sysmon-raw_score 1 ]lac:lDate17708803809765. TimeCreated: /Date/1770803437769, Date: 2022

□ Message File created: RuleName: - UtcTime: 2026-02-10 06:14:14:132 ProcessGuid: [redacted]
  ProcessId: 3392 Image: C:\Users\demo\AppData\Local\Microsoft\OneDrive\26.087.011.082\Microsoft.Edge\1129.111.Taks.exe TargetTantFle C:Vindow1Sydem23\GTh
  TimeCreated: /date/17706844744997 _id 2I7633i73A4h4)38: 6gmore ProviderName Microsoft-Windows-Sysmon
```

MITRE ATT&CK: Technique Mapping

Technique	Technique ID
Command Shell Execution	T1059.003
PowerShell Execution	T1059.001
Modify Registry	T1112
Boot or Logon Autostart — Registry Run Keys	T1547.001
OS Credential Dumping (LSASS)	T1003.001
Application Layer Protocol — Web (C2)	T1071.001

Risk Scoring Matrix

Behavior	Severity (1-10)	Impact Level
PowerShell Execution	6	Medium
Registry Deletion	8	High
LSASS Interaction	9	Critical
Outbound Network Activity	7	High
Multi-Event Correlation	10	Critical

False Positive Analysis

Potential benign scenarios include legitimate administrative PowerShell execution, Windows update services modifying registry keys, antivirus interaction with *L*sass.exe, or standard applications such as browsers and OneDrive generating outbound HTTPS (TCP 443) traffic. Individually, each of these activities may occur during normal system operations and therefore cannot be classified as malicious without additional contextual validation.

However, the observed events occurred in a tightly correlated sequence within a short time window: command shell spawing PowerShell, ed., immediate RunOnce registry modification (T1112, T1547.001), suspicious file staging in the Temp directory, access to the LSASS process (T1003.001), and outbound encrypted HTTPS communication via TCP 443 (T1071.001). The structured behavioral alignment across eẋecution (T1059.003, T1059.001), registry modification (T1112, T1547.001), credential dumping (T1003.001), and command-and-control (C2) traffic (T1071.001) significantly reduces false positive likelihood, strongly suggesting malicious pre-encryption ransomware staging rather than isolated legitimate system behavior.

Incident Response Report

Incident Type: Suspected Pre-Ransomware Staging Activity

Severity Level: Critical

Incident Summary:

Correlated multi-stage behavior was observed within a short time window, including command shell execution, PowerShell spawning, registry persistence modification (RunOnce), suspicious file creation in the Temp directory, LSASS process interaction, and outbound encrypted communication over TCP 443. The sequential behavioral alignment indicates potential ransomware pre-encryption preparation rather than isolated benign activity.

Recommended Actions:

- Immediately isolate the affected host from the network to prevent lateral movement
- Capture volatile memory for forensic analysis prior to system shutdown
- Reset affected and potentially exposed user credentials
- Block and investigate suspicious external IP addresses at the firewall level
- Review and remove unauthorized persistence mechanisms (RunOnce keys, start-up. entries)
- Conduct full EDR scan and comprehensive malware analysis
- Initiate proactive threat hunting across the environment for similar indicators

Conclusion

This project demonstrates advanced SOC-level behavioral detection engineering using real-world telemetry from Sysmon logs. By leveraging multi-event correlation rather than single IOC alerts, this approach enables early detection of ransomware staging behavior before encryption impact occurs.

The methodology highlights proactive defense strategy, detection tuning, false positive reduction, and structured incident response planning.