DuCharme Triage Assistant
Analysis Report

Report Generated: 2026-02-13 13:31:11

1) FILE INFORMATION

Property	Value
File Name	NewDirtySecurity.evtx
File Path	C:/Users/colli/Downloads/Skewel/PortableGit/logparser
File Size	1092.00 KB
Analysis Date	2026-02-13 13:31:11

2) ASSET & SCOPE

Property	Value
Affected System:	CROBZPC
Operating System:	Not detected in logs
User Accounts:	*1 unique user account(s) detected* **1 Regular User(s):** colli
Network Connections:	No external network activity detected
Domain/Workgroup:	WORKGROUP
How System Was Accessed:	Network file/printer access, Automated tasks/services
Evidence Sources:	Security

Analysis Timeframe:	2026-02-13 17:25:16 to 2026-02-13 17:29:26 *Total Events Analyzed: 99*

3) INCIDENT CONTEXT (INPUT)

Field	Information
How was this incident reported?	Joe
What was observed?	computer stuff
Suspected cause (if known)	bad stuff
Impact on business/operations	idk

4) TIMELINE (LAST N DAYS)

Total Events with Timestamps: 99
Time Windows (5 min intervals): 1
Time Span: 2026-02-13 17:25 to 2026-02-13 17:29

First 15 Events (Chronological)

#	Timestamp	Event ID
1	2026-02-13 17:25:16	1102
2	2026-02-13 17:27:22	4624
3	2026-02-13 17:27:22	4672
4	2026-02-13 17:29:19	4625
5	2026-02-13 17:29:19	4625
6	2026-02-13 17:29:20	4625
7	2026-02-13 17:29:20	4625
8	2026-02-13 17:29:21	4625
9	2026-02-13 17:29:21	4728
10	2026-02-13 17:29:21	4720
11	2026-02-13 17:29:21	4722

12	2026-02-13 17:29:21	4738
13	2026-02-13 17:29:21	4724
14	2026-02-13 17:29:21	4732
15	2026-02-13 17:29:21	4798

Top 5 Busiest Time Windows

Rank	Time Window	Event Count	Top Event IDs
1	2026-02-13 17:25	99	5379(71), 4625(5), 4738(4)

5) INDICATORS & SCORING (SUMMARY)

Category: Defense Evasion

Indicator: Security Logs Cleared

CVSS Score: 9.0

Evidence (1-line): Event ID 1102 occurred 1 time(s)

Category: Privilege Escalation

Indicator: User Added to Privileged Group

CVSS Score: 8.0

Evidence (1-line): Event ID 4732 occurred 1 time(s)

Category: Credential Access

Indicator: Failed Login Attempt

CVSS Score: 7.0

Evidence (1-line): Event ID 4625 occurred 5 time(s)

Category: Privilege Escalation

Indicator: User Added to Global Group

CVSS Score: 7.0

Evidence (1-line): Event ID 4728 occurred 1 time(s)

Category: Persistence

Indicator: User Account Created

CVSS Score: 7.0

Evidence (1-line): Event ID 4720 occurred 1 time(s)

Category: Persistence

Indicator: User Account Enabled

CVSS Score: 6.0

Evidence (1-line): Event ID 4722 occurred 2 time(s)

Category: Persistence

Indicator: User Account Changed

CVSS Score: 6.0

Evidence (1-line): Event ID 4738 occurred 4 time(s)

Category: Defense Evasion

Indicator: User Account Deleted

CVSS Score: 5.0

Evidence (1-line): Event ID 4726 occurred 1 time(s)

Highest CVSS Score: 9.0 → **Risk Level:** Critical

Generated by DuCharme Triage Assistant on 2026-02-13 13:31:11