DuCharme Triage Assistant Analysis Report

Report Generated: 2026-02-13 13:30:20

1) FILE INFORMATION

Property	Value
File Name	DirtySysmon.evtx
File Path	C:/Users/colli/Downloads/Skewel/PortableGit/logparser
File Size	1092.00 KB
Analysis Date	2026-02-13 13:30:20

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):** CROBZPC\colli
Network Connections:	1.1.1.1, 10.23.4.121, 162.159.135.232
Domain/Workgroup:	WORKGROUP
How System Was Accessed:	No login activity detected
Evidence Sources:	Sysmon

Analysis Timeframe:	2026-01-18 17:51:53 to 2026-01-18 18:19:55 *Total Events Analyzed: 365*

3) INCIDENT CONTEXT (INPUT)

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

4) TIMELINE (LAST N DAYS)

Total Events with Timestamps: 365
Time Windows (5 min intervals): 6
Time Span: 2026-01-18 17:51 to 2026-01-18 18:19

First 15 Events (Chronological)

#	Timestamp	Event ID
1	2026-01-18 17:51:53	16
2	2026-01-18 17:51:53	4
3	2026-01-18 17:51:53	1
4	2026-01-18 17:51:53	1
5	2026-01-18 17:51:54	5
6	2026-01-18 17:52:58	5
7	2026-01-18 17:53:05	5
8	2026-01-18 17:53:08	1
9	2026-01-18 17:53:12	5
10	2026-01-18 17:54:00	1
11	2026-01-18 17:54:00	1

12	2026-01-18 17:54:00	5
13	2026-01-18 17:54:06	1
14	2026-01-18 17:54:06	1
15	2026-01-18 17:54:28	5

Top 5 Busiest Time Windows

Rank	Time Window	Event Count	Top Event IDs
1	2026-01-18 17:55	138	5(73), 1(65)
2	2026-01-18 18:15	65	1(38), 5(12), 22(7)
3	2026-01-18 18:00	54	5(30), 1(24)
4	2026-01-18 18:05	45	5(24), 1(21)
5	2026-01-18 18:10	36	1(18), 5(18)

5) INDICATORS & SCORING (SUMMARY)

Category: Execution

Indicator: Suspicious Process Creation

CVSS Score: 9.0

Evidence (1-line): Event ID 1 occurred 180 time(s)

Category: Command and Control

Indicator: Outbound Connection to Suspicious IP

CVSS Score: 8.0

Evidence (1-line): Event ID 3 occurred 4 time(s)

Category: Command and Control

Indicator: DNS Query to Malicious Domain

CVSS Score: 7.0

Evidence (1-line): Event ID 22 occurred 7 time(s)

Category: Execution

Indicator: File Created in Suspicious Location

CVSS Score: 6.0

Evidence (1-line): Event ID 11 occurred 3 time(s)

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

Generated by DuCharme Triage Assistant on 2026-02-13 13:30:20