

DuCharme Triage Assistant

Analysis Report

Report Generated: 2026-02-13 13:32:13

1) FILE INFORMATION

Property	Value
File Name	DirtySystem.evtx
File Path	C:/Users/collie/Downloads/Skewel/PortableGit/logparser
File Size	1092.00 KB
Analysis Date	2026-02-13 13:32:13

2) ASSET & SCOPE

Property	Value
Affected System:	CROBZPC
Operating System:	Windows 11 (Build 26100)
User Accounts:	No human user activity detected in logs
Network Connections:	No external network activity detected
Domain/Workgroup:	WORKGROUP
How System Was Accessed:	No login activity detected
Evidence Sources:	System
Analysis Timeframe:	2026-02-13 17:32:24 to 2026-02-13 18:19:22 <i>Total Events Analyzed: 167</i>

3) INCIDENT CONTEXT (INPUT)

Field	Information
How was this incident reported?	Nathan
What was observed?	malicious service
Suspected cause (if known)	hackers
Impact on business/operations	stolen data

4) TIMELINE (LAST N DAYS)

Total Events with Timestamps: 167

Time Windows (5 min intervals): 4

Time Span: 2026-02-13 17:32 to 2026-02-13 18:19

First 15 Events (Chronological)

#	Timestamp	Event ID
1	2026-02-13 17:32:24	104
2	2026-02-13 17:34:49	7045
3	2026-02-13 17:34:54	7045
4	2026-02-13 17:34:55	7045
5	2026-02-13 17:34:56	7045
6	2026-02-13 17:38:47	6009
7	2026-02-13 17:38:47	6005
8	2026-02-13 17:38:47	6013
9	2026-02-13 18:13:21	7040
10	2026-02-13 18:15:25	7040
11	2026-02-13 18:17:18	1074
12	2026-02-13 18:17:23	7002
13	2026-02-13 18:17:23	2

14	2026-02-13 18:17:34	50104
15	2026-02-13 18:17:34	51047

Top 5 Busiest Time Windows

Rank	Time Window	Event Count	Top Event IDs
1	2026-02-13 18:15	158	6(17), 112(16), 16(13)
2	2026-02-13 17:30	5	7045(4), 104(1)
3	2026-02-13 17:35	3	6009(1), 6005(1), 6013(1)
4	2026-02-13 18:10	1	7040(1)

5) INDICATORS & SCORING (SUMMARY)

Category: Persistence

Indicator: Suspicious Service Installed

CVSS Score: 9.0

Evidence (1-line): Event ID 7045 occurred 4 time(s)

Category: Execution

Indicator: Suspicious Process Creation

CVSS Score: 9.0

Evidence (1-line): Event ID 1 occurred 9 time(s)

Category: Credential Access

Indicator: LSASS Memory Access

CVSS Score: 9.0

Evidence (1-line): Event ID 10 occurred 1 time(s)

Category: Command and Control

Indicator: Outbound Connection to Suspicious IP

CVSS Score: 8.0

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

Category: Persistence

Indicator: Driver Loaded

CVSS Score: 8.0

Evidence (1-line): Event ID 6 occurred 17 time(s)

Category: Impact

Indicator: Mass File Deletion

CVSS Score: 8.0

Evidence (1-line): Event ID 23 occurred 1 time(s)

Category: Defense Evasion

Indicator: File Timestamp Modified

CVSS Score: 7.0

Evidence (1-line): Event ID 2 occurred 3 time(s)

Category: Persistence

Indicator: Registry Persistence Mechanism

CVSS Score: 7.0

Evidence (1-line): Event ID 13 occurred 1 time(s)

Category: Persistence

Indicator: Registry Object Modified

CVSS Score: 6.0

Evidence (1-line): Event ID 12 occurred 3 time(s)

Category: Execution

Indicator: Named Pipe Connected

CVSS Score: 5.0

Evidence (1-line): Event ID 18 occurred 4 time(s)

Category: Execution

Indicator: Named Pipe Created

CVSS Score: 5.0

Evidence (1-line): Event ID 17 occurred 1 time(s)

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

Generated by DuCharme Triage Assistant on 2026-02-13 13:32:13