FORENSIC LOG ANALYSIS REPORT

Case: demo for the logs

Status: OPEN

Generated: 2026-01-14 11:18:36 UTC

Generated By: hno2

CHAIN OF CUSTODY

All evidence files have been cryptographically hashed (SHA-256) to ensure integrity.

Filename	SHA-256 Hash	Upload Time	Uploader
botsv3_events.csv	74b5606d02344d1d...	2026-01-14 11:00:59	hno2

EXECUTIVE SUMMARY

As a senior cybersecurity forensic analyst, my analysis o...

Attack Phase: UNKNOWN

As a senior cybersecurity forensic analyst, my analysis of the provided security events indicates a potential multi-stage

Our analysis indicates a multi-stage intrusion, likely in...

Attack Phase: UNKNOWN

Our analysis indicates a multi-stage intrusion, likely initiated through a compromised user account, followed by

TIMELINE OF EVENTS

[2026-01-11 08:15:00] 4688 - *CRITICAL*

[2026-01-11 08:15:00] 4688 - *CRITICAL*

[2026-01-11 15:15:05] 4625 - *CRITICAL*

[2026-01-11 15:15:05] 4625 - *CRITICAL*

[2026-01-11 15:17:30] 4688 - *CRITICAL*

[2026-01-11 15:18:00] 5156 - *CRITICAL*

[2026-01-11 15:19:30] 5156 - *CRITICAL*

[2026-01-11 15:17:30] 4688 - *CRITICAL*

[2026-01-11 15:18:00] 5156 - *CRITICAL*

[2026-01-11 15:19:30] 5156 - *CRITICAL*

[2026-01-11 23:05:00] 4634 - *HIGH*

[2026-01-11 23:05:00] 4634 - *HIGH*

[2026-01-11 08:12:00] 4624 - *HIGH*

[2026-01-11 09:00:00] 4663 - *HIGH*

[2026-01-11 08:12:00] 4624 - *HIGH*

[2026-01-11 10:15:00] 4624 - *HIGH*

[2026-01-11 11:10:00] 4663 - *HIGH*

[2026-01-11 09:00:00] 4663 - *HIGH*

[2026-01-11 10:15:00] 4624 - *HIGH*

[2026-01-11 11:10:00] 4663 - *HIGH*

[2026-01-11 15:10:00] 4663 - *HIGH*

[2026-01-11 15:15:00] 4625 - *HIGH*

[2026-01-11 15:15:10] 4625 - *HIGH*

[2026-01-11 15:15:15] 4625 - *HIGH*

[2026-01-11 15:15:20] 4625 - *HIGH*

[2026-01-11 15:15:30] 4625 - *HIGH*

[2026-01-11 15:15:35] 4625 - *HIGH*

[2026-01-11 15:16:00] 4625 - *HIGH*

[2026-01-11 15:16:05] 4625 - *HIGH*

[2026-01-11 15:16:15] 4625 - *HIGH*

[2026-01-11 15:16:20] 4625 - *HIGH*

[2026-01-11 15:16:25] 4625 - *HIGH*

[2026-01-11 15:16:30] 4625 - *HIGH*

[2026-01-11 15:10:00] 4663 - *HIGH*

[2026-01-11 15:15:00] 4625 - *HIGH*

[2026-01-11 15:15:10] 4625 - *HIGH*

[2026-01-11 15:15:15] 4625 - *HIGH*

[2026-01-11 15:15:20] 4625 - *HIGH*

[2026-01-11 15:15:30] 4625 - *HIGH*

[2026-01-11 15:17:00] 4624 - *HIGH*

[2026-01-11 15:18:30] 4663 - *HIGH*

[2026-01-11 15:19:00] 4688 - *HIGH*

[2026-01-11 15:20:00] 4719 - *HIGH*

[2026-01-11 15:21:00] 4688 - *HIGH*

[2026-01-11 15:15:35] 4625 - *HIGH*

[2026-01-11 15:16:00] 4625 - *HIGH*

[2026-01-11 15:16:05] 4625 - *HIGH*

[2026-01-11 15:16:15] 4625 - *HIGH*

[2026-01-11 15:16:20] 4625 - *HIGH*

[2026-01-11 15:16:25] 4625 - *HIGH*

DETAILED EVIDENCE

Time	Event Type	Confidence	Risk	Details
01/11 08:15	4688	0.80	CRITICAL	timestamp=2026-01-11 08:15:00 | event_id=4688 | so...
01/11 08:15	4688	0.80	CRITICAL	timestamp=2026-01-11 08:15:00 | event_id=4688 | so...
01/11 15:15	4625	0.80	CRITICAL	timestamp=2026-01-11 15:15:05 | event_id=4625 | so...
01/11 15:15	4625	0.80	CRITICAL	timestamp=2026-01-11 15:15:05 | event_id=4625 | so...
01/11 15:17	4688	0.80	CRITICAL	timestamp=2026-01-11 15:17:30 | event_id=4688 | so...
01/11 15:18	5156	0.80	CRITICAL	timestamp=2026-01-11 15:18:00 | event_id=5156 | so...
01/11 15:19	5156	0.80	CRITICAL	timestamp=2026-01-11 15:19:30 | event_id=5156 | so...
01/11 15:17	4688	0.80	CRITICAL	timestamp=2026-01-11 15:17:30 | event_id=4688 | so...
01/11 15:18	5156	0.80	CRITICAL	timestamp=2026-01-11 15:18:00 | event_id=5156 | so...
01/11 15:19	5156	0.80	CRITICAL	timestamp=2026-01-11 15:19:30 | event_id=5156 | so...
01/11 23:05	4634	0.80	HIGH	timestamp=2026-01-11 23:05:00 | event_id=4634 | so...
01/11 23:05	4634	0.80	HIGH	timestamp=2026-01-11 23:05:00 | event_id=4634 | so...
01/11 08:12	4624	0.70	HIGH	timestamp=2026-01-11 08:12:00 | event_id=4624 | so...
01/11 09:00	4663	0.70	HIGH	timestamp=2026-01-11 09:00:00 | event_id=4663 | so...
01/11 08:12	4624	0.70	HIGH	timestamp=2026-01-11 08:12:00 | event_id=4624 | so...
01/11 10:15	4624	0.70	HIGH	timestamp=2026-01-11 10:15:00 | event_id=4624 | so...
01/11 11:10	4663	0.70	HIGH	timestamp=2026-01-11 11:10:00 | event_id=4663 | so...
01/11 09:00	4663	0.70	HIGH	timestamp=2026-01-11 09:00:00 | event_id=4663 | so...
01/11 10:15	4624	0.70	HIGH	timestamp=2026-01-11 10:15:00 | event_id=4624 | so...
01/11 11:10	4663	0.70	HIGH	timestamp=2026-01-11 11:10:00 | event_id=4663 | so...
01/11 15:10	4663	0.70	HIGH	timestamp=2026-01-11 15:10:00 | event_id=4663 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:00 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:10 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:15 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:20 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:30 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:35 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:00 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:05 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:15 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:20 | event_id=4625 | so...

01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:25 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:30 | event_id=4625 | so...
01/11 15:10	4663	0.70	HIGH	timestamp=2026-01-11 15:10:00 | event_id=4663 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:00 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:10 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:15 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:20 | event_id=4625 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:30 | event_id=4625 | so...
01/11 15:17	4624	0.70	HIGH	timestamp=2026-01-11 15:17:00 | event_id=4624 | so...
01/11 15:18	4663	0.70	HIGH	timestamp=2026-01-11 15:18:30 | event_id=4663 | so...
01/11 15:19	4688	0.70	HIGH	timestamp=2026-01-11 15:19:00 | event_id=4688 | so...
01/11 15:20	4719	0.70	HIGH	timestamp=2026-01-11 15:20:00 | event_id=4719 | so...
01/11 15:21	4688	0.70	HIGH	timestamp=2026-01-11 15:21:00 | event_id=4688 | so...
01/11 15:15	4625	0.70	HIGH	timestamp=2026-01-11 15:15:35 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:00 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:05 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:15 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:20 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:25 | event_id=4625 | so...
01/11 15:16	4625	0.70	HIGH	timestamp=2026-01-11 15:16:30 | event_id=4625 | so...
01/11 15:17	4624	0.70	HIGH	timestamp=2026-01-11 15:17:00 | event_id=4624 | so...
01/11 15:18	4663	0.70	HIGH	timestamp=2026-01-11 15:18:30 | event_id=4663 | so...
01/11 15:19	4688	0.70	HIGH	timestamp=2026-01-11 15:19:00 | event_id=4688 | so...
01/11 15:20	4719	0.70	HIGH	timestamp=2026-01-11 15:20:00 | event_id=4719 | so...
01/11 15:21	4688	0.70	HIGH	timestamp=2026-01-11 15:21:00 | event_id=4688 | so...
01/11 20:50	4688	0.70	HIGH	timestamp=2026-01-11 20:50:00 | event_id=4688 | so...
01/11 20:50	4688	0.70	HIGH	timestamp=2026-01-11 20:50:00 | event_id=4688 | so...
01/11 20:25	4663	0.60	HIGH	timestamp=2026-01-11 20:25:00 | event_id=4663 | so...
01/11 20:25	4663	0.60	HIGH	timestamp=2026-01-11 20:25:00 | event_id=4663 | so...
01/11 22:00	4688	0.50	MEDIUM	timestamp=2026-01-11 22:00:00 | event_id=4688 | so...
01/11 22:05	5156	0.50	MEDIUM	timestamp=2026-01-11 22:05:00 | event_id=5156 | so...
01/11 22:10	4663	0.50	MEDIUM	timestamp=2026-01-11 22:10:00 | event_id=4663 | so...
01/11 22:15	4688	0.50	MEDIUM	timestamp=2026-01-11 22:15:00 | event_id=4688 | so...
01/11 22:20	5156	0.50	MEDIUM	timestamp=2026-01-11 22:20:00 | event_id=5156 | so...
01/11 22:25	4663	0.50	MEDIUM	timestamp=2026-01-11 22:25:00 | event_id=4663 | so...

01/11 22:30	4688	0.50	MEDIUM	timestamp=2026-01-11 22:30:00 | event_id=4688 | so...
01/11 22:35	4663	0.50	MEDIUM	timestamp=2026-01-11 22:35:00 | event_id=4663 | so...
01/11 22:40	5156	0.50	MEDIUM	timestamp=2026-01-11 22:40:00 | event_id=5156 | so...
01/11 22:45	4688	0.50	MEDIUM	timestamp=2026-01-11 22:45:00 | event_id=4688 | so...
01/11 22:50	4663	0.50	MEDIUM	timestamp=2026-01-11 22:50:00 | event_id=4663 | so...
01/11 22:55	4719	0.50	MEDIUM	timestamp=2026-01-11 22:55:00 | event_id=4719 | so...
01/11 23:00	4688	0.50	MEDIUM	timestamp=2026-01-11 23:00:00 | event_id=4688 | so...
01/11 23:10	5156	0.50	MEDIUM	timestamp=2026-01-11 23:10:00 | event_id=5156 | so...
01/11 23:15	4663	0.50	MEDIUM	timestamp=2026-01-11 23:15:00 | event_id=4663 | so...
01/11 23:20	4688	0.50	MEDIUM	timestamp=2026-01-11 23:20:00 | event_id=4688 | so...
01/11 23:25	4663	0.50	MEDIUM	timestamp=2026-01-11 23:25:00 | event_id=4663 | so...
01/11 23:30	5156	0.50	MEDIUM	timestamp=2026-01-11 23:30:00 | event_id=5156 | so...
01/11 23:35	4663	0.50	MEDIUM	timestamp=2026-01-11 23:35:00 | event_id=4663 | so...
01/11 23:40	4688	0.50	MEDIUM	timestamp=2026-01-11 23:40:00 | event_id=4688 | so...
01/11 23:45	4719	0.50	MEDIUM	timestamp=2026-01-11 23:45:00 | event_id=4719 | so...
01/11 23:50	5156	0.50	MEDIUM	timestamp=2026-01-11 23:50:00 | event_id=5156 | so...
01/11 23:55	4663	0.50	MEDIUM	timestamp=2026-01-11 23:55:00 | event_id=4663 | so...
01/11 23:59	4688	0.50	MEDIUM	timestamp=2026-01-11 23:59:00 | event_id=4688 | so...
01/11 23:59	4663	0.50	MEDIUM	timestamp=2026-01-11 23:59:30 | event_id=4663 | so...
01/11 23:59	4902	0.50	MEDIUM	timestamp=2026-01-11 23:59:59 | event_id=4902 | so...
01/11 22:00	4688	0.50	MEDIUM	timestamp=2026-01-11 22:00:00 | event_id=4688 | so...
01/11 22:05	5156	0.50	MEDIUM	timestamp=2026-01-11 22:05:00 | event_id=5156 | so...
01/11 22:10	4663	0.50	MEDIUM	timestamp=2026-01-11 22:10:00 | event_id=4663 | so...
01/11 22:15	4688	0.50	MEDIUM	timestamp=2026-01-11 22:15:00 | event_id=4688 | so...
01/11 22:20	5156	0.50	MEDIUM	timestamp=2026-01-11 22:20:00 | event_id=5156 | so...
01/11 22:25	4663	0.50	MEDIUM	timestamp=2026-01-11 22:25:00 | event_id=4663 | so...
01/11 22:30	4688	0.50	MEDIUM	timestamp=2026-01-11 22:30:00 | event_id=4688 | so...
01/11 22:35	4663	0.50	MEDIUM	timestamp=2026-01-11 22:35:00 | event_id=4663 | so...
01/11 22:40	5156	0.50	MEDIUM	timestamp=2026-01-11 22:40:00 | event_id=5156 | so...
01/11 22:45	4688	0.50	MEDIUM	timestamp=2026-01-11 22:45:00 | event_id=4688 | so...
01/11 22:50	4663	0.50	MEDIUM	timestamp=2026-01-11 22:50:00 | event_id=4663 | so...
01/11 22:55	4719	0.50	MEDIUM	timestamp=2026-01-11 22:55:00 | event_id=4719 | so...
01/11 23:00	4688	0.50	MEDIUM	timestamp=2026-01-11 23:00:00 | event_id=4688 | so...
01/11 23:10	5156	0.50	MEDIUM	timestamp=2026-01-11 23:10:00 | event_id=5156 | so...