Incident Response Report

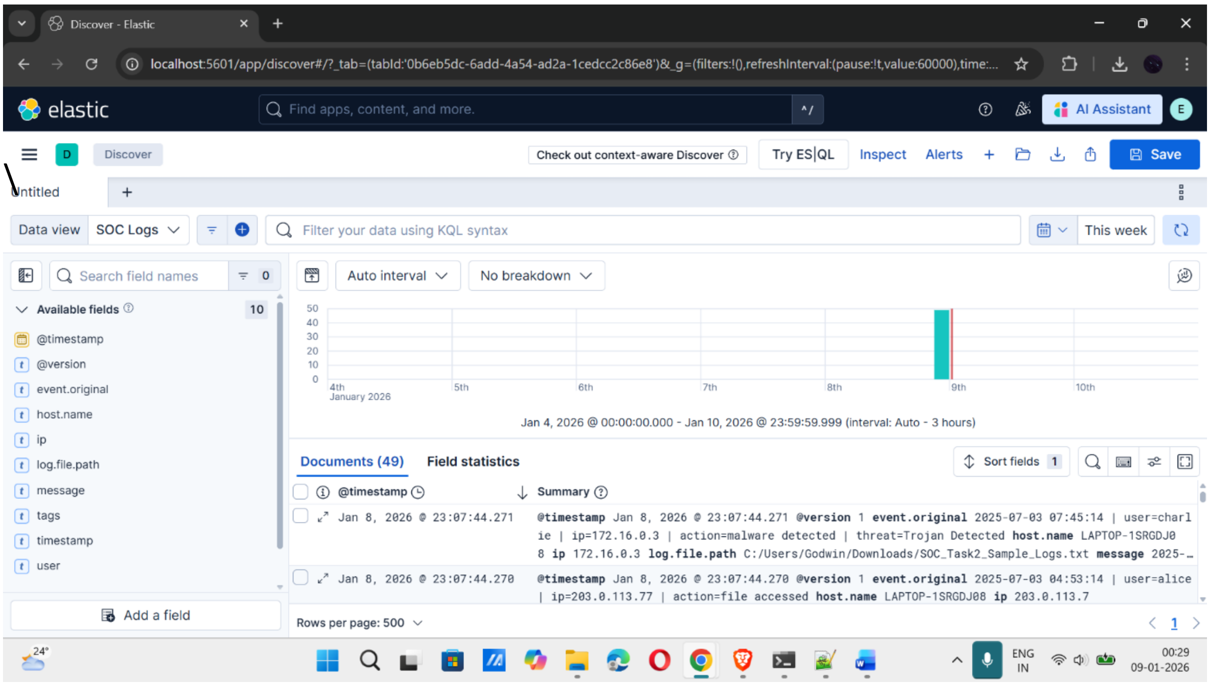
1. Executive Summary

During monitoring using the Elastic Stack (SIEM), multiple high-risk security alerts were detected across several user accounts and IP addresses. The alerts indicated malware infections like, Trojans, Worms, Rootkits, and Ransomware behaviour, combined with repeated authentication failures.

Further analysis confirmed a multi-host malware incident with possible credential compromise.

2. Environment Overview

- **SIEM Tool Used:** Elastic Stack (Elasticsearch + Kibana + Logstash)
- **Log Source:** Simulated SOC logs (SOC_Task2_Sample_Logs)
- **Index Name:** soc-logs
- **Log Types Analysed:**
  - Authentication logs
  - Network connection logs
  - Malware detection alerts
  - File access logs



localhost:5601/app/discover#/?_tab=(tabId:'0b6eb5dc-6add-4a54-ad2a-1cedcc2c86e8')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:...

Data view: SOC Logs

Jan 4, 2026 @ 00:00:00.000 - Jan 10, 2026 @ 23:59:59.999 (interval: Auto - 3 hours)

Documents (49)

```
@timestamp                    Summary
Jan 8, 2026 @ 23:07:44.271    @timestamp Jan 8, 2026 @ 23:07:44.271 @version 1 event.original 2025-07-03 07:45:14 | user=charl
                              ie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected host.name LAPTOP-1SRGDJ0
                              8 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-…
Jan 8, 2026 @ 23:07:44.270    @timestamp Jan 8, 2026 @ 23:07:44.270 @version 1 event.original 2025-07-03 04:53:14 | user=alice
                              | ip=203.0.113.77 | action=file accessed host.name LAPTOP-1SRGDJ08 ip 203.0.113.7
```

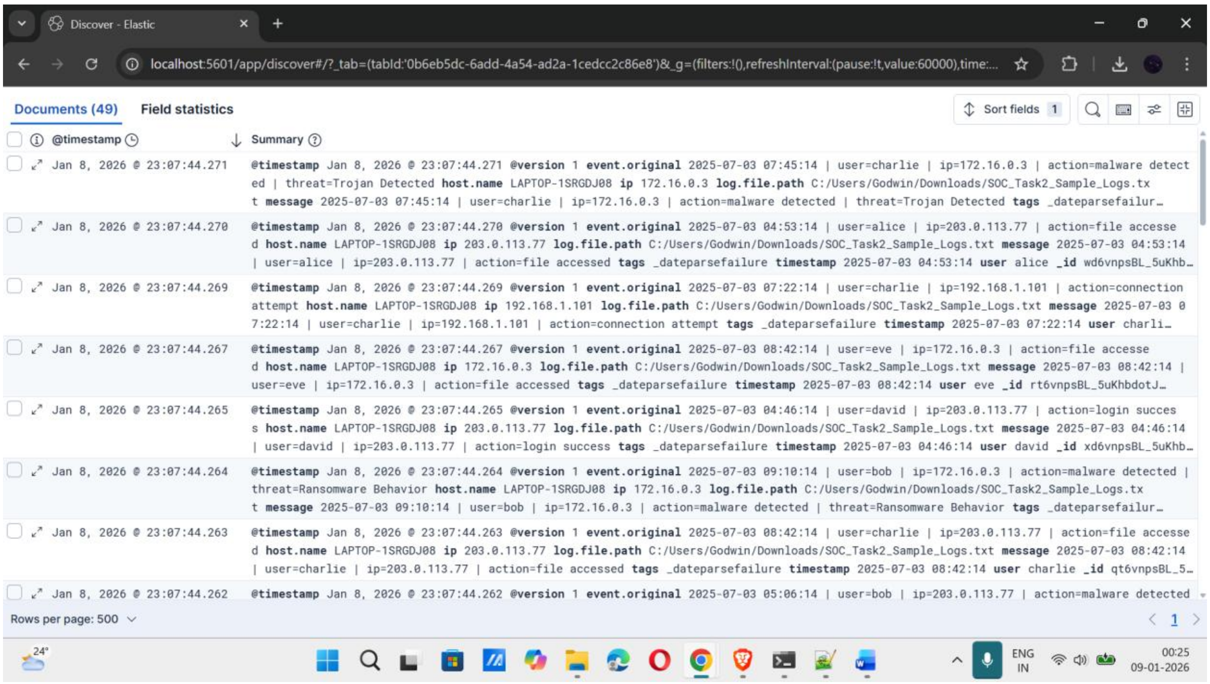
Rows per page: 500

3. Incident Detection

The incident was detected through automated SIEM ingestion and manual analysis in Kibana. Alerts triggered included:

- Malware detection events
- Multiple failed login attempts
- Suspicious IP activity across multiple users

These alerts were reviewed in the **Discover** section of Kibana.


Discover - Elastic
localhost:5601/app/discover#/?_tab=(tabId:'0b6eb5dc-6add-4a54-ad2a-1cedcc2c86e8')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:...
Documents (49)
Field statistics
Sort fields 1
@timestamp
Summary
Rows per page: 500
1
24°
ENG
IN
00:25
09-01-2026

```
Jan 8, 2026 @ 23:07:44.271   @timestamp Jan 8, 2026 @ 23:07:44.271 @version 1 event.original 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detect
                             ed | threat=Trojan Detected host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.tx
                             t message 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected tags _dateparsefailur…
Jan 8, 2026 @ 23:07:44.270   @timestamp Jan 8, 2026 @ 23:07:44.270 @version 1 event.original 2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 04:53:14
                             | user=alice | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 04:53:14 user alice _id wd6vnpsBL_5uKhb…
Jan 8, 2026 @ 23:07:44.269   @timestamp Jan 8, 2026 @ 23:07:44.269 @version 1 event.original 2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection
                             attempt host.name LAPTOP-1SRGDJ08 ip 192.168.1.101 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 0
                             7:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt tags _dateparsefailure timestamp 2025-07-03 07:22:14 user charli…
Jan 8, 2026 @ 23:07:44.267   @timestamp Jan 8, 2026 @ 23:07:44.267 @version 1 event.original 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 08:42:14 |
                             user=eve | ip=172.16.0.3 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 08:42:14 user eve _id rt6vnpsBL_5uKhbdotJ…
Jan 8, 2026 @ 23:07:44.265   @timestamp Jan 8, 2026 @ 23:07:44.265 @version 1 event.original 2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login succes
                             s host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 04:46:14
                             | user=david | ip=203.0.113.77 | action=login success tags _dateparsefailure timestamp 2025-07-03 04:46:14 user david _id xd6vnpsBL_5uKhb…
Jan 8, 2026 @ 23:07:44.264   @timestamp Jan 8, 2026 @ 23:07:44.264 @version 1 event.original 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected |
                             threat=Ransomware Behavior host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.tx
                             t message 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior tags _dateparsefailur…
Jan 8, 2026 @ 23:07:44.263   @timestamp Jan 8, 2026 @ 23:07:44.263 @version 1 event.original 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 08:42:14
                             | user=charlie | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 08:42:14 user charlie _id qt6vnpsBL_5…
Jan 8, 2026 @ 23:07:44.262   @timestamp Jan 8, 2026 @ 23:07:44.262 @version 1 event.original 2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected
```

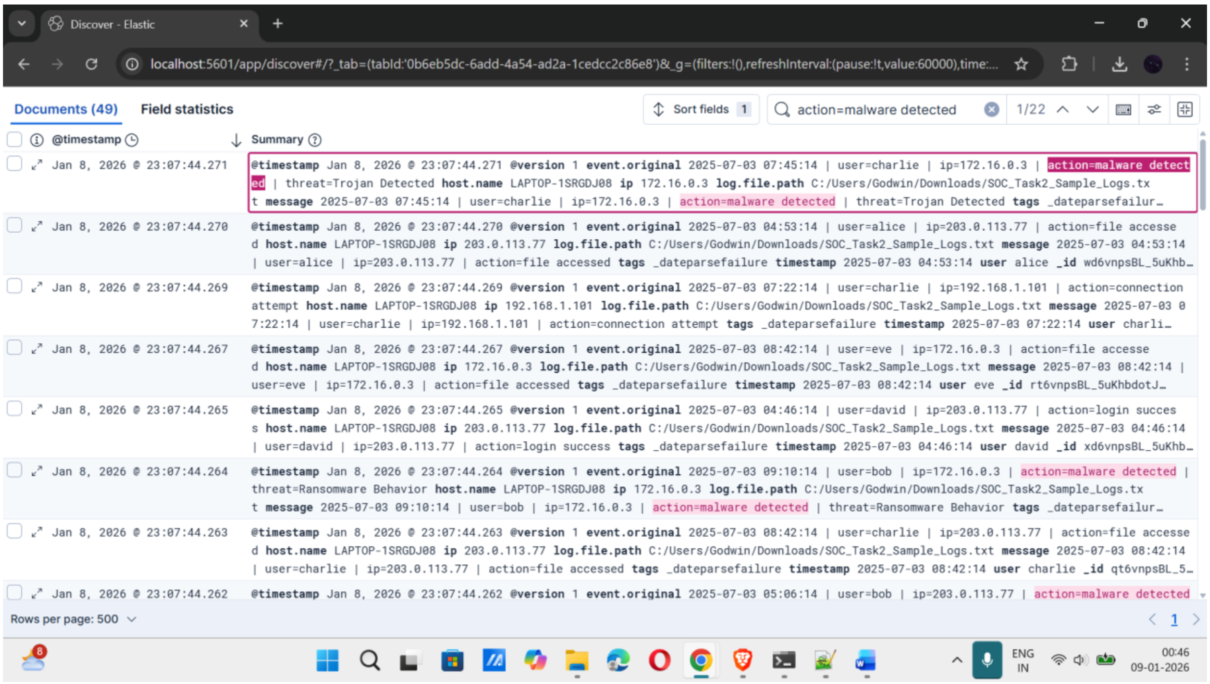
4. Identified Suspicious Activities

4.1 Malware Infections (High Severity)

The following malware related alerts were identified:

- Trojan detections on multiple hosts
- Rootkit signature alerts
- Worm infection attempts
- Ransomware behaviour detection

These alerts indicate active system compromise rather than beginning activity.


Discover - Elastic
localhost:5601/app/discover#/?_tab=(tabId:'0b6eb5dc-6add-4a54-ad2a-1cedcc2c86e8')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:...
Documents (49)
Field statistics
Sort fields 1
1/22
@timestamp
Summary
Rows per page: 500
1
ENG
IN
00:46
09-01-2026

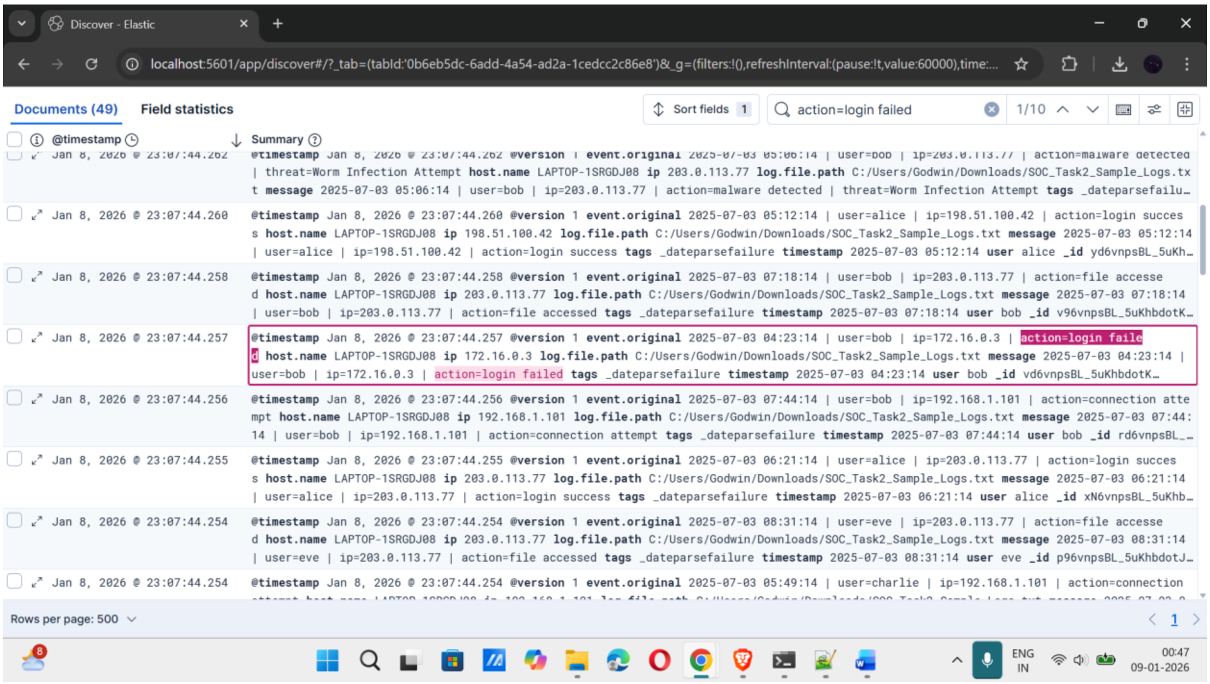
action=malware detected

```
Jan 8, 2026 @ 23:07:44.271   @timestamp Jan 8, 2026 @ 23:07:44.271 @version 1 event.original 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detect
                             ed | threat=Trojan Detected host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.tx
                             t message 2025-07-03 07:45:14 | user=charlie | ip=172.16.0.3 | action=malware detected | threat=Trojan Detected tags _dateparsefailur…
Jan 8, 2026 @ 23:07:44.270   @timestamp Jan 8, 2026 @ 23:07:44.270 @version 1 event.original 2025-07-03 04:53:14 | user=alice | ip=203.0.113.77 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 04:53:14
                             | user=alice | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 04:53:14 user alice _id wd6vnpsBL_5uKhb…
Jan 8, 2026 @ 23:07:44.269   @timestamp Jan 8, 2026 @ 23:07:44.269 @version 1 event.original 2025-07-03 07:22:14 | user=charlie | ip=192.168.1.101 | action=connection
                             attempt host.name LAPTOP-1SRGDJ08 ip 192.168.1.101 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 0
                             7:22:14 | user=charlie | ip=192.168.1.101 | action=connection attempt tags _dateparsefailure timestamp 2025-07-03 07:22:14 user charli…
Jan 8, 2026 @ 23:07:44.267   @timestamp Jan 8, 2026 @ 23:07:44.267 @version 1 event.original 2025-07-03 08:42:14 | user=eve | ip=172.16.0.3 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 08:42:14 |
                             user=eve | ip=172.16.0.3 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 08:42:14 user eve _id rt6vnpsBL_5uKhbdotJ…
Jan 8, 2026 @ 23:07:44.265   @timestamp Jan 8, 2026 @ 23:07:44.265 @version 1 event.original 2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login succes
                             s host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 04:46:14
                             | user=david | ip=203.0.113.77 | action=login success tags _dateparsefailure timestamp 2025-07-03 04:46:14 user david _id xd6vnpsBL_5uKhb…
Jan 8, 2026 @ 23:07:44.264   @timestamp Jan 8, 2026 @ 23:07:44.264 @version 1 event.original 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected |
                             threat=Ransomware Behavior host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.tx
                             t message 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior tags _dateparsefailur…
Jan 8, 2026 @ 23:07:44.263   @timestamp Jan 8, 2026 @ 23:07:44.263 @version 1 event.original 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 08:42:14
                             | user=charlie | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 08:42:14 user charlie _id qt6vnpsBL_5…
Jan 8, 2026 @ 23:07:44.262   @timestamp Jan 8, 2026 @ 23:07:44.262 @version 1 event.original 2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected
```

4.2 Authentication Abuse (Medium to High Severity)

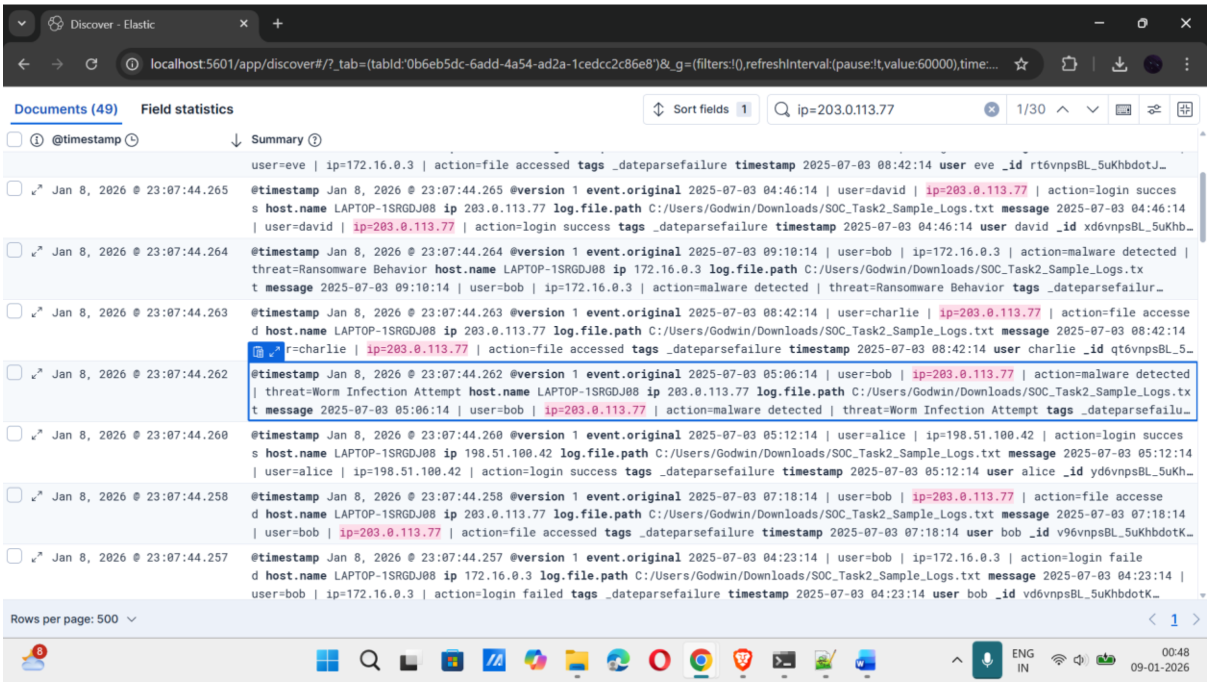
- Multiple failed login attempts from the same IP addresses
- Failed login attempts followed by successful access
- Same IPs associated with malware alerts

This behaviour suggests credential brute-force attempts or compromised credentials.


Discover - Elastic
localhost:5601/app/discover#/?_tab=(tabId:'0b6eb5dc-6add-4a54-ad2a-1cedcc2c86e8')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:...
Documents (49)
Field statistics
Sort fields 1
1/10
@timestamp
Summary
Rows per page: 500
1
ENG
IN
00:47
09-01-2026

action=login failed

```
Jan 8, 2026 @ 23:07:44.262   @timestamp Jan 8, 2026 @ 23:07:44.262 @version 1 event.original 2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected
                             | threat=Worm Infection Attempt host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.tx
                             t message 2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt tags _dateparsefailu…
Jan 8, 2026 @ 23:07:44.260   @timestamp Jan 8, 2026 @ 23:07:44.260 @version 1 event.original 2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login succes
                             s host.name LAPTOP-1SRGDJ08 ip 198.51.100.42 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 05:12:14
                             | user=alice | ip=198.51.100.42 | action=login success tags _dateparsefailure timestamp 2025-07-03 05:12:14 user alice _id yd6vnpsBL_5uKh…
Jan 8, 2026 @ 23:07:44.258   @timestamp Jan 8, 2026 @ 23:07:44.258 @version 1 event.original 2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 07:18:14
                             | user=bob | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 07:18:14 user bob _id v96vnpsBL_5uKhbdotK…
Jan 8, 2026 @ 23:07:44.257   @timestamp Jan 8, 2026 @ 23:07:44.257 @version 1 event.original 2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login faile
                             d host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 04:23:14 |
                             user=bob | ip=172.16.0.3 | action=login failed tags _dateparsefailure timestamp 2025-07-03 04:23:14 user bob _id vd6vnpsBL_5uKhbdotK…
Jan 8, 2026 @ 23:07:44.256   @timestamp Jan 8, 2026 @ 23:07:44.256 @version 1 event.original 2025-07-03 07:44:14 | user=bob | ip=192.168.1.101 | action=connection atte
                             mpt host.name LAPTOP-1SRGDJ08 ip 192.168.1.101 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 07:44:
                             14 | user=bob | ip=192.168.1.101 | action=connection attempt tags _dateparsefailure timestamp 2025-07-03 07:44:14 user bob _id rd6vnpsBL_…
Jan 8, 2026 @ 23:07:44.255   @timestamp Jan 8, 2026 @ 23:07:44.255 @version 1 event.original 2025-07-03 06:21:14 | user=alice | ip=203.0.113.77 | action=login succes
                             s host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 06:21:14
                             | user=alice | ip=203.0.113.77 | action=login success tags _dateparsefailure timestamp 2025-07-03 06:21:14 user alice _id xN6vnpsBL_5uKhb…
Jan 8, 2026 @ 23:07:44.254   @timestamp Jan 8, 2026 @ 23:07:44.254 @version 1 event.original 2025-07-03 08:31:14 | user=eve | ip=203.0.113.77 | action=file accesse
                             d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 08:31:14
                             | user=eve | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 08:31:14 user eve _id p96vnpsBL_5uKhbdotJ…
Jan 8, 2026 @ 23:07:44.254   @timestamp Jan 8, 2026 @ 23:07:44.254 @version 1 event.original 2025-07-03 05:49:14 | user=charlie | ip=192.168.1.101 | action=connection
```


Discover - Elastic
localhost:5601/app/discover#/?_tab=(tabId:'0b6eb5dc-6add-4a54-ad2a-1cedcc2c86e8')&_g=(filters:!(),refreshInterval:(pause:!t,value:60000),time:...
Documents (49)
Field statistics
Sort fields 1
ip=203.0.113.77
1/30
@timestamp
Summary
Rows per page: 500
1
ENG
IN
00:48
09-01-2026

```
                                user=eve | ip=172.16.0.3 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 08:42:14 user eve _id rt6vnpsBL_5uKhbdotJ…
Jan 8, 2026 @ 23:07:44.265     @timestamp Jan 8, 2026 @ 23:07:44.265 @version 1 event.original 2025-07-03 04:46:14 | user=david | ip=203.0.113.77 | action=login succes
                                s host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 04:46:14
                                | user=david | ip=203.0.113.77 | action=login success tags _dateparsefailure timestamp 2025-07-03 04:46:14 user david _id xd6vnpsBL_5uKhb…
Jan 8, 2026 @ 23:07:44.264     @timestamp Jan 8, 2026 @ 23:07:44.264 @version 1 event.original 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected |
                                threat=Ransomware Behavior host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.tx
                                t message 2025-07-03 09:10:14 | user=bob | ip=172.16.0.3 | action=malware detected | threat=Ransomware Behavior tags _dateparsefailur…
Jan 8, 2026 @ 23:07:44.263     @timestamp Jan 8, 2026 @ 23:07:44.263 @version 1 event.original 2025-07-03 08:42:14 | user=charlie | ip=203.0.113.77 | action=file accesse
                                d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 08:42:14
                                r=charlie | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 08:42:14 user charlie _id qt6vnpsBL_5…
Jan 8, 2026 @ 23:07:44.262     @timestamp Jan 8, 2026 @ 23:07:44.262 @version 1 event.original 2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected
                                | threat=Worm Infection Attempt host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.tx
                                t message 2025-07-03 05:06:14 | user=bob | ip=203.0.113.77 | action=malware detected | threat=Worm Infection Attempt tags _dateparsefailu…
Jan 8, 2026 @ 23:07:44.260     @timestamp Jan 8, 2026 @ 23:07:44.260 @version 1 event.original 2025-07-03 05:12:14 | user=alice | ip=198.51.100.42 | action=login succes
                                s host.name LAPTOP-1SRGDJ08 ip 198.51.100.42 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 05:12:14
                                | user=alice | ip=198.51.100.42 | action=login success tags _dateparsefailure timestamp 2025-07-03 05:12:14 user alice _id yd6vnpsBL_5uKh…
Jan 8, 2026 @ 23:07:44.258     @timestamp Jan 8, 2026 @ 23:07:44.258 @version 1 event.original 2025-07-03 07:18:14 | user=bob | ip=203.0.113.77 | action=file accesse
                                d host.name LAPTOP-1SRGDJ08 ip 203.0.113.77 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 07:18:14
                                | user=bob | ip=203.0.113.77 | action=file accessed tags _dateparsefailure timestamp 2025-07-03 07:18:14 user bob _id v96vnpsBL_5uKhbdotK…
Jan 8, 2026 @ 23:07:44.257     @timestamp Jan 8, 2026 @ 23:07:44.257 @version 1 event.original 2025-07-03 04:23:14 | user=bob | ip=172.16.0.3 | action=login faile
                                d host.name LAPTOP-1SRGDJ08 ip 172.16.0.3 log.file.path C:/Users/Godwin/Downloads/SOC_Task2_Sample_Logs.txt message 2025-07-03 04:23:14 |
                                user=bob | ip=172.16.0.3 | action=login failed tags _dateparsefailure timestamp 2025-07-03 04:23:14 user bob _id vd6vnpsBL_5uKhbdotK…
```

4.3 Suspicious IP Addresses

The following IPs were involved in multiple malicious activities:

- 203.0.113.77
- 172.16.0.3
- 10.0.0.5
- 198.51.100.42

These IPs were flagged as high-risk.

5. Incident Classification

Category	Details
Incident Type	Malware Infection & Credential Compromise
Severity	High
Scope	Multiple users and systems
Status	Contained (Simulated)

6. Incident Timeline (Simplified)

1. Initial malware detection alerts triggered
2. Multiple failed login attempts observed
3. Repeated activity from same IPs across users
4. File access events after malware detection
5. Incident confirmed and escalated

7. Impact Assessment

- Potential compromise of multiple endpoints
- Risk of unauthorized access and data exposure
- Possible lateral movement inside the environment
- Business operations at risk if incident were real

8. Incident Response Actions (Simulated)

8.1 Containment

- Isolating affected systems
- Blocking malicious IP addresses
- Temporarily disabling compromised user accounts

8.2 Eradication

- Initiating full malware scans
- Removing detected threats
- Resetting credentials for affected users

8.3 Recovery

- Verifying system integrity
- Restoring normal operations
- Continuing monitoring for recurrence

9. Recommendations

- Enforce strong password policies and MFA
- Improve SIEM alert tuning
- Implement endpoint detection and response (EDR)
- Conduct regular security awareness training
- Monitor high-risk IP ranges proactively

10. Conclusion

The investigation successfully identified and classified a high-severity security incident involving malware and authentication abuse. Proper SOC procedures were followed, and recommended actions were documented to prevent future occurrences.