

# **Incident Response Report**

**-By Using SIEM Tools**

## **Table Of Contents:**

- 1.Incident Summary
- 2.Detection Method(Includes Tools Used)
- 3.Procedure
4. Alert Summary Table
5. Incident Timeline
- 6.Affected Entities(Includes Screen Shots)
- 7.Impact Analysis
- 8.Recommendations
- 9.Conclusion

## **Incident Title - Trojan Malware Detection**

### **1. Incident Summary:-**

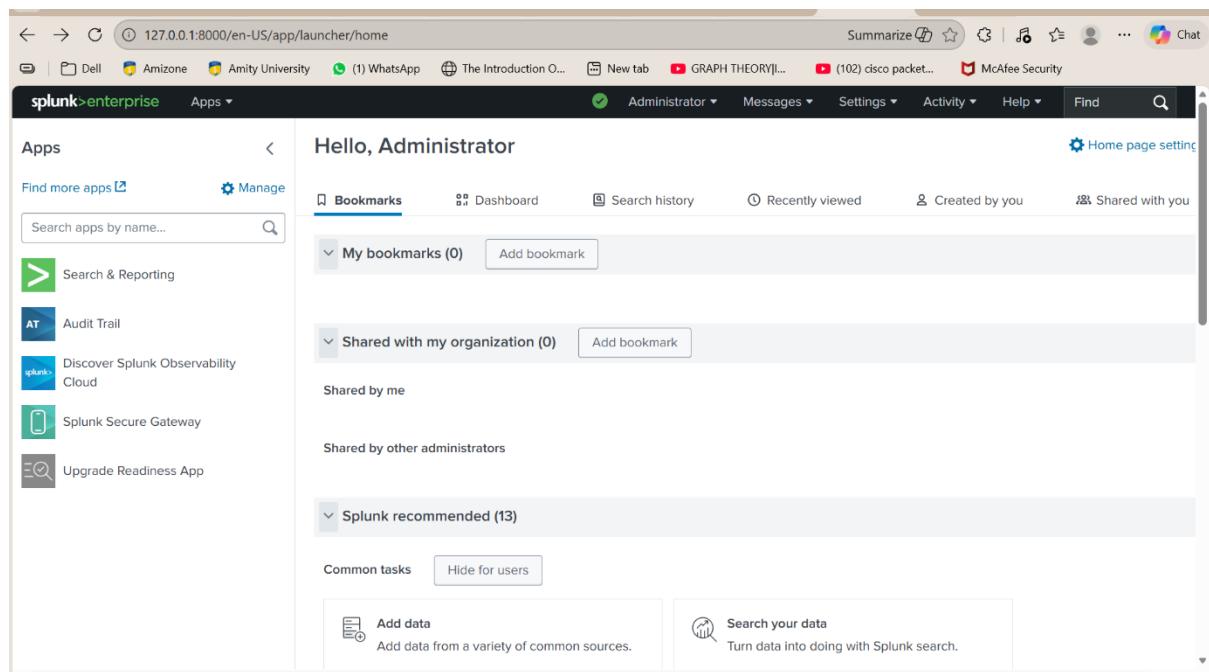
Multiple malware detection alerts indicating Trojan activity were observed in the system logs. These alerts were detected across different users and IP addresses, suggesting a potential malware infection within the environment.

### **2. Detection Method:-**

The incident was detected through SIEM log analysis using Splunk, by filtering events where the action field indicated malware detected and the threat type was Trojan Detected.

### **3. Procedure:-**

#### **3.1. Splunk was set up as the SIEM tool for log analysis.**



The screenshot shows the Splunk Enterprise web interface. The top navigation bar includes links for 'Dell', 'Amizone', 'Amity University', '(1) WhatsApp', 'The Introduction O...', 'New tab', 'GRAPH THEORY...', '(102) cisco packet...', and 'McAfee Security'. The main header says 'splunk>enterprise' and 'Hello, Administrator'. The left sidebar lists 'Apps' such as 'Search & Reporting', 'Audit Trail', 'Discover Splunk Observability Cloud', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. The right side features sections for 'Bookmarks' (empty), 'Dashboard', 'Search history', 'Recently viewed', 'Created by you', and 'Shared with you'. Below these are sections for 'My bookmarks (0)', 'Shared with my organization (0)', 'Splunk recommended (13)', 'Common tasks' (with 'Add data' and 'Search your data' options), and 'Hide for users'.

#### **3.2. Sample log files were uploaded into Splunk and indexed successfully.**

The screenshot shows the Splunk Add Data interface at the 'Select Source' step. The URL is 127.0.0.1:8000/en-US/manager/search/adddatamethods/selectsource?input\_mode=0. The top navigation bar includes links like Dell, Amizone, Amity University, WhatsApp, The Introduction O..., New tab, GRAPH THEORY!..., (102) cisco packet..., McAfee Security, and a Chat icon. The main header says 'splunk>enterprise Apps'. Below it, a progress bar shows 'Add Data' with five steps: 'Select Source' (green dot), 'Set Source Type' (white dot), 'Input Settings' (white dot), 'Review' (white dot), and 'Done' (white dot). A 'Next >' button is highlighted in green. The main content area is titled 'Select Source' and instructs users to choose a file to upload. It shows a selected file 'SOC\_Task2\_Sample\_Logs.txt' and a 'Select File' button. There's a large input field labeled 'Drop your data file here' with a note that the maximum file upload size is 500 Mb. A success message 'File Successfully Uploaded' is displayed with a checkmark icon. At the bottom, there's an 'FAQ' section.

3.3. Log analysis was performed by defining source, index, and host parameters, making the data ready for security queries.

The screenshot shows the Splunk Add Data interface at the 'success' step. The URL is 127.0.0.1:8000/en-US/manager/search/adddatamethods/success. The top navigation bar and header are identical to the previous screenshot. The progress bar now shows all five steps ('Select Source', 'Set Source Type', 'Input Settings', 'Review', 'Done') with green dots and checkmarks. A 'Next >' button is also present. The main content area displays a success message: '✓ File has been uploaded successfully.' It also says 'Configure your inputs by going to Settings > Data Inputs'. Below this, there are several buttons with descriptions: 'Start Searching' (Search your data now or see examples and tutorials.), 'Extract Fields' (Create search-time field extractions. Learn more about fields.), 'Add More Data' (Add more data inputs now or see examples and tutorials.), 'Download Apps' (Apps help you do more with your data. Learn more.), and 'Build Dashboards' (Visualize your searches. Learn more.).

3.4. Malware Detection Query:

```
source="SOC_Task2_Sample_Logs.txt" host="HARSHA" index="main"  
sourcetype="soc_sample_logs" action="malware detected"
```

source="SOC\_Task2\_Sample\_Logs.txt" host="HARSHA" index="main" sourcetype="soc\_sample\_logs" action="malware detected"

✓ 11 events (before 12/24/25 6:43:13.000 PM) No Event Sampling ▾

Events (11) Patterns Statistics Visualization

Timeline format ▾ – Zoom Out + Zoom to Selection × Deselect

Format ▾ Show: 20 Per Page ▾ View: List ▾

Time	Event
7/3/25 9:10:14.000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
7/3/25 7:51:14.000 AM	2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
7/3/25 7:45:14.000 AM	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
7/3/25 5:48:14.000 AM	2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs

## 4. Alert Summary Table:-

Alert ID	Alert Type	Severity	Log Source
A-01	Trojan Malware Detected	High	Endpoint Logs
A-02	Multiple Login Failures	Medium	Authentication Logs
A-03	Unusual IP Activity	Medium	Network Logs

## 5. Incident Timeline

Time (Approx.)	Activity
09:04	Malware detection alert triggered in SIEM
09:10	SOC analyst reviewed logs and identified Trojan activity
09:20	Incident classified as High severity
09:30	Recommended containment and remediation actions documented

## 6. Affected Entities:-

- Users:** bob, eve, charlie, alice
- IP addresses:** 172.16.0.3, 203.0.113.77, 10.0.0.5, 192.168.1.101

Format ▾ Show: 20 Per Page ▾ View: List ▾

i	Time	Event
>	7/3/25 9:10:14.000 AM	2025-07-03 09:10:14   user=bob   ip=172.16.0.3   action=malware detected   threat=Ransomware Behavior host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 7:51:14.000 AM	2025-07-03 07:51:14   user=eve   ip=10.0.0.5   action=malware detected   threat=Rootkit Signature host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 7:45:14.000 AM	2025-07-03 07:45:14   user=charlie   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:48:14.000 AM	2025-07-03 05:48:14   user=bob   ip=10.0.0.5   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:45:14.000 AM	2025-07-03 05:45:14   user=david   ip=172.16.0.3   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:42:14.000 AM	2025-07-03 05:42:14   user=eve   ip=203.0.113.77   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:30:14.000 AM	2025-07-03 05:30:14   user=eve   ip=192.168.1.101   action=malware detected   threat=Trojan Detected host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 5:06:14.000 AM	2025-07-03 05:06:14   user=bob   ip=203.0.113.77   action=malware detected   threat=Worm Infection Attempt host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs
>	7/3/25 4:41:14.000 AM	2025-07-03 04:41:14   user=alice   ip=172.16.0.3   action=malware detected   threat=Spyware Alert host = HARSHA   source = SOC_Task2_Sample_Logs.txt   sourcetype = soc_sample_logs

- **Severity Level:-High**

## 7. Impact Analysis:-

Trojan malware can allow unauthorized access, data theft, and further malware installation. If left unaddressed, this could lead to system compromise and data loss.

## 8. Recommended Actions

- Isolate affected systems from the network
- Perform malware scans and removal
- Reset compromised user credentials
- Monitor network traffic for suspicious activity
- Apply security patches and updates

## 9. Conclusion:-

The investigation confirmed multiple high-severity malware alerts indicating Trojan activity across several user accounts and IP addresses. The detected behaviour suggests a potential system compromise that could lead to unauthorized access, data theft, or further malware spread if left unmitigated. Based on the analysis, the incident was classified as High severity and requires immediate containment and remediation actions. Continuous monitoring and improved security controls are recommended to prevent similar incidents in the future.

