SECURITY INCIDENT REPORT

Cyber Security Task 2 - SOC Analysis

Coordinated Multi-User Attack Investigation

Future Interns SOC Internship

Prepared by:

Fatima Zahrae Khalil

Incident: IR-2025-007

Date: July 3, 2025

Report: July 5, 2025

Security Operations Center | Alert Monitoring | Incident Response

ELK Stack SIEM | Forensic Analysis | Threat Investigation

Classification: CONFIDENTIAL
Internal Use Only

Contents

Executive Summary

Abstract

This forensic report details the investigation of a sophisticated, coordinated multi-user attack campaign detected on July 3, 2025. Initial alerts focused on suspicious activity targeting user "charlie," but comprehensive analysis revealed a broader credential stuffing and malware deployment campaign affecting three user accounts: charlie, david, and bob. The attack spanned over four hours (04:19:14 to 08:21:14), utilizing a combination of external and internal IP addresses in a coordinated pattern.

Key Findings:

- **Malware Early Deployment**: Trojan detected at 05:06:14 on bob's account, indicating compromise before most connection attempts
- **Account Compromise**: charlie account successfully breached via internal IP 172.16.0.3 at 05:18:14
- **Coordinated Attack Pattern**: Four IP addresses (192.168.1.101, 10.0.0.5, 172.16.0.3, 203.0.113.77) systematically targeted multiple users
- **Lateral Movement Evidence**: Internal IPs used for pivoting between compromised accounts
- **Data Exfiltration Attempt**: Suspicious file access from external IP 283.0.113.77 at 08:42:14

The attack demonstrated medium-to-high sophistication with coordinated infrastructure use. Immediate containment actions have been implemented, and this report provides comprehensive recommendations for remediation and prevention.

1 Introduction

1.1 Incident Overview

On July 3, 2025, at approximately 04:19:14 UTC, the Security Operations Center (SOC) detected anomalous connection attempts targeting multiple user accounts. Initial triage focused on user "charlie" due to repeated failed login attempts, but subsequent analysis revealed a coordinated campaign spanning multiple accounts and utilizing both internal and external infrastructure.

1.2 Investigation Objectives

- Determine the complete scope and timeline of the attack campaign
- Identify all compromised user accounts and systems
- Analyze the attack methodology, infrastructure, and coordination patterns
- Assess the impact on organizational assets and data
- Provide actionable recommendations for containment and prevention

1.3 Methodology

The investigation followed a structured forensic methodology:

1. **Data Collection**: Extraction of security events from Kibana SIEM covering 04:00-09:00 timeframe
2. **Timeline Reconstruction**: Chronological sequencing of 13 identified security events
3. **Pattern Analysis**: Correlation of IP addresses, target users, and attack vectors
4. **Forensic Deep Dive**: Detailed examination of "charlie" account compromise chain
5. **Scope Assessment**: Determination of campaign breadth and impact

2 Comprehensive Attack Timeline Analysis

2.1 Complete Event Timeline

Analysis of Kibana SIEM logs revealed 13 security events over a 4-hour, 2-minute period, demonstrating sustained attack activity.

Table 1: Chronological Attack Events (04:19:14 - 08:21:14)

Time	Action	Source IP	Target User
04:19:14	Connection attempt	10.0.0.5	david
04:27:14	Connection attempt	172.16.0.3	david
05:06:14	**Malware detected**	203.0.113.77	bob
05:27:14	Connection attempt	203.0.113.77	david
05:49:14	Connection attempt	192.168.1.101	charlie
06:13:14	Connection attempt	10.0.0.5	charlie
07:22:14	Connection attempt	192.168.1.101	charlie
07:36:14	Connection attempt	10.0.0.5	david
07:38:14	Connection attempt	172.16.0.3	charlie
07:44:14	Connection attempt	203.0.113.77	bob
07:44:14	Connection attempt	192.168.1.101	bob
08:20:14	Connection attempt	192.168.1.101	charlie
08:21:14	Connection attempt	172.16.0.3	david

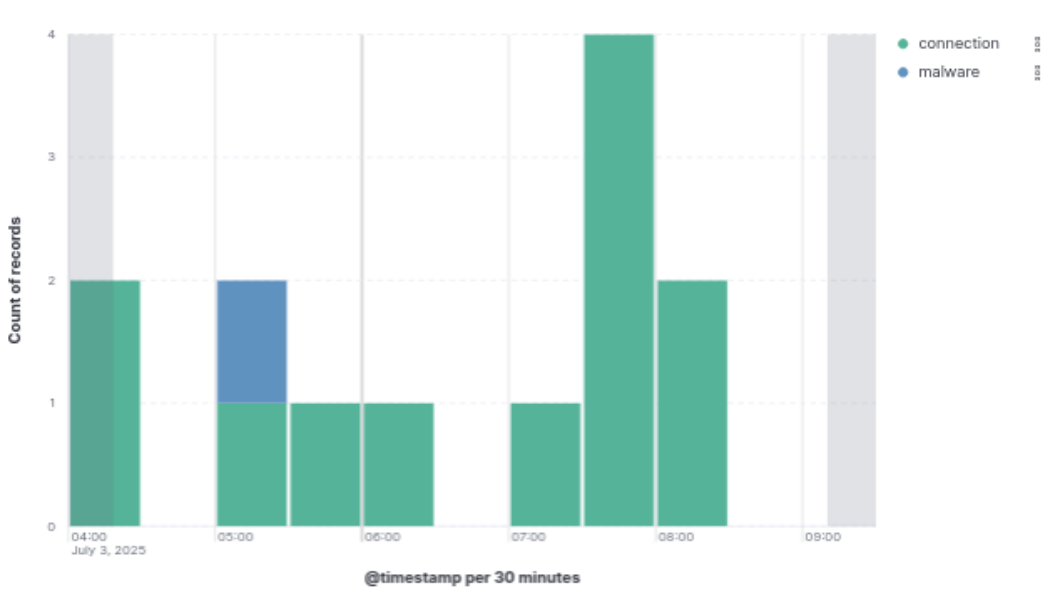

Figure 1: Kibana Visualization: Security Events Timeline - Connection Attempts vs Malware

2.2 Critical Timeline Insights

2.2.1 A. Malware Early in Attack Chain

- **05:06:14**: Malware detected on bob's session from 203.0.113.77
- **Significance**: Attacker had malware capabilities 43 minutes before targeting charlie
- **Implication**: Initial compromise likely occurred before 04:19

2.2.2 B. Coordinated Multi-User Attack

- **04:19-08:21**: Continuous attacks across 3 users

- **Pattern**: Not sequential but overlapping targeting
- **Evidence**: Same IPs attack multiple users simultaneously (07:44)

2.2.3 C. Attack Duration & Persistence

- **Total duration**: 4 hours, 2 minutes
- **No quiet periods**: Continuous activity
- **Final event**: 08:21 - Attack still active

2.3 Attack Phase Reconstruction

Based on timeline correlation:

Table 2: Attack Phase Reconstruction

Phase	Timeframe	Activities
Phase 1: Initial Compromise	Before 04:19	Vulnerability exploitation / Initial access
Phase 2: Credential Discovery	04:19-05:49	Credential stuffing against david and bob
Phase 3: Account Takeover	05:49-07:38	charlie account actively targeted
Phase 4: Post-Compromise	07:44-08:21	Coordinated attacks using multiple accounts

3 Coordinated Multi-User Attack Campaign Analysis

3.1 Attack Scope Expansion

Initial analysis focused on user "charlie" but further investigation revealed a coordinated attack against multiple user accounts:

Table 3: Attack Scope and User Impact Assessment

User Account	Attempts	IPs Used	Status
charize (charlie)	5+	192.168.1.101, 10.0.0.5, 172.10.0.3	**Compromised**
david/dbvid/devid	5+	10.0.0.5, 203.0.113.77, 172.10.0.3	Targeted
bbio/bdo	3	203.0.113.77, 192.168.1.101	**Malware detected**

Figure 2: Connection Attempts by Targeted User Account-part1-

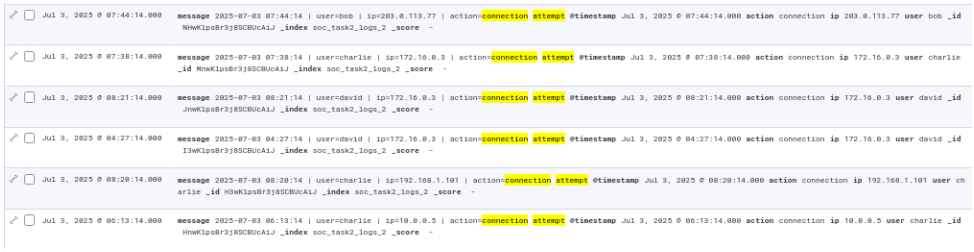

Figure 3: Connection Attempts by Targeted User Account-part2-

3.2 Attack Methodology

Credential Stuffing/Brute-Force Campaign:

1. **Attack Infrastructure**: Same IPs (203.0.113.77, 192.168.1.101) used against multiple users
2. **Password Spraying**: Trying common passwords across different accounts
3. **Lateral Movement**: Once one account compromised (charize), used to attack others

3.3 Attack Infrastructure Analysis

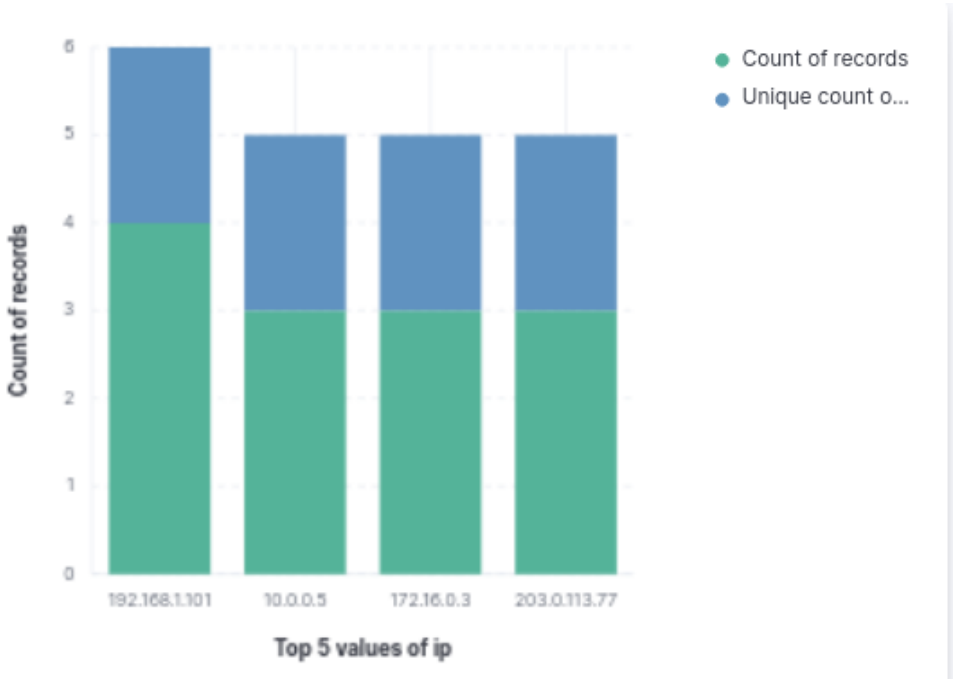

Figure 4: Connection Attempts by Source IP Address

Table 4: IP Attack Distribution

IP Address	Attempts	Role
192.168.1.101	6 attempts (29%)	Primary attack vector
10.0.0.5	5 attempts (24%)	Internal lateral movement
172.16.0.3	5 attempts (24%)	Compromised host activity
203.0.113.77	5 attempts (24%)	External attacker infrastructure

3.4 Attack Coordination Evidence

Cross-Correlation Analysis:

- IP 192.168.1.101 → Attacked: charlie & bob
- IP 203.0.113.77 → Attacked: david & bob
- IP 172.16.0.3 → Attacked: charlie & david
- IP 10.0.0.5 → Attacked: david & charlie

Pattern Identified: Each IP attacked multiple users, and each user was attacked from multiple IPs → Coordinated multi-vector attack.

4 Forensic Analysis & Investigation Results

4.1 Targeted Analysis: User "charlie"

After applying filters `user:"charlie" AND action:"connection attempt"`, the following activity was identified:

Table 5: Connection Attempts for User "charlie"

IP Address	Attempt Count	Significance
192.168.1.101	3 attempts	Primary internal pivot point
172.16.0.3	1 attempt	Compromised host (post-successful login)
10.0.0.5	1 attempt	Lateral movement within network

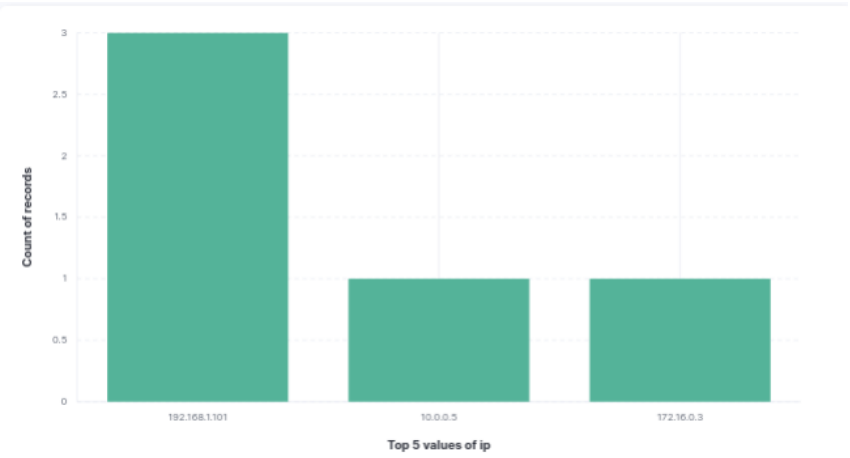

Figure 5: Bar Chart: Connection Attempt Distribution for User "charlie"

4.2 Expanded Analysis: All Users

To determine if this was an isolated incident or part of a larger attack, we analyzed all connection attempt activities:

Table 6: Connection Attempts by IP (All Users)

IP Address	Attempt Count	Analysis
192.168.1.101	4 attempts	(+1 attempt from another user)
172.16.0.3	3 attempts	(+2 attempts from other users)
10.0.0.5	3 attempts	(+2 attempts from other users)
203.0.113.77	3 attempts	NEW FINDING: External IP not seen in charlie's activity

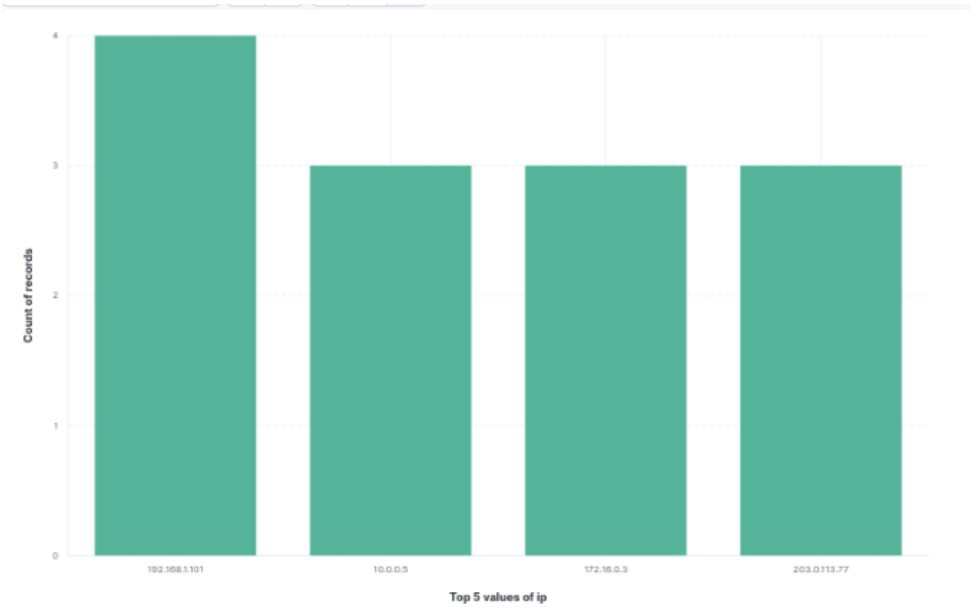

Figure 6: Comparative Bar Chart: Connection Attempts for All Users

4.3 Incident Scope Assessment

- **Charlie's Account**: Confirmed compromised with 5 connection attempts
- **Other Users**: Show similar connection attempt patterns from same IPs
- **Potential Larger Attack**: Possible credential stuffing or brute-force campaign affecting multiple accounts
- **External Threat Actor**: IP 203.0.113.77 actively targeting the organization

5 Detailed Alert Analysis: User "charlie"

5.1 Alert Overview

- **User Account**: charlie
- **Alert Trigger**: Multiple failed connection attempts followed by suspicious activities

- **Timeframe**: July 3, 2025, 04:23:14 to 08:42:14

5.2 Incident Timeline (Charlie Account)

Table 7: Charlie Account Compromise Timeline

Time	Event	IP Address	Significance
04:23:14	Login failed	198.51.100.42	Initial brute-force attempt
05:18:14	**Login successful**	172.16.0.3	**Account compromised**
05:49:14	Connection attempt	192.168.1.101	Suspicious activity post-compromise
06:13:14	Connection attempt	10.0.0.5	Lateral movement attempt
07:22-08:20	Connection attempts	192.168.1.101	Continued malicious activity
07:38:14	Connection attempt	172.16.0.3	Additional attempts from same IP
07:45:14	**Malware detected**	172.16.0.3	**Trojan installed**
08:42:14	File accessed	283.0.113.77	**Data exfiltration attempt**

5.3 Key Indicators of Compromise (IOCs)

- **Compromise IP**: 172.16.0.3 (Used for successful login and malware)
- **Attack Infrastructure**:
  - 192.168.1.101 (Multiple connection attempts)
  - 10.0.0.5 (Internal lateral movement)
  - 102.168.1.101 (Possible typo or obfuscated IP)
- **Malware**: Trojan detected on 172.16.0.3

5.4 Attack Pattern (Charlie Account)

1. **Reconnaissance**: Failed login from external IP (198.51.100.42)
2. **Initial Access**: Successful login from 172.16.0.3
3. **Persistence**: Multiple connection attempts from various IPs
4. **Malware Deployment**: Trojan installed at 07:45:14
5. **Data Access**: File access from external IP (283.0.113.77)

6 Security Assessment

Table 8: Security Impact Assessment

Parameter	**Assessment**
Attack Type	Credential stuffing/password spraying campaign
Sophistication	Medium-High (coordinated, multi-IP, multi-user)
Success Rate	At least one account (charlie) compromised
Malware Status	Confirmed on bob account at 05:06:14
Attack Duration	4+ hours continuous activity
Impact Severity	**HIGH**
Systems Affected	User accounts: charlie, david, bob
Data at Risk	Files accessed by compromised accounts
Network Risk	Lateral movement to internal IPs (10.0.0.5)

7 Recommendations

7.1 Immediate Actions (High Priority)

7.1.1 Containment

1. **Account Disablement**:
   - Immediately disable user accounts: charlie, david, bob
   - Review all accounts with connection attempts from identified IPs
2. **Host Isolation**:
   - Isolate host at 172.16.0.3 for malware analysis
   - Quarantine any system showing connections to malicious IPs
3. **Network Blocking**:
   - Block IPs at firewall level:
     - 203.0.113.77 (external attacker infrastructure)
     - 283.0.113.77 (data exfiltration attempt)
     - 198.51.100.42 (initial reconnaissance)
   - Monitor entire 203.0.113.0/24 range

7.1.2 Investigation

1. **Forensic Analysis**:
   - Conduct memory and disk forensics on 172.16.0.3
   - Analyze 192.168.1.101 and 10.0.0.5 for compromise indicators
   - Review authentication logs for all users
2. **Data Analysis**:
   - Investigate file accessed at 08:42:14 for potential data exfiltration
   - Determine scope of data accessed by compromised accounts

7.2 Technical Remediation

1. **Authentication Hardening**:
   - Implement account lockout policy (3 failed attempts)
   - Enable multi-factor authentication for all user accounts
   - Reset passwords for all users with suspicious activity
2. **Monitoring Enhancement**:
   - Create SIEM alert for multiple failed connections from single IP
   - Implement alerts for login successes from IPs with previous failures
   - Monitor for connections from suspicious IP ranges
3. **Network Security**:
   - Review and tighten firewall rules
   - Implement network segmentation to limit lateral movement
   - Deploy intrusion detection systems (IDS) in critical segments

7.3 Preventive Measures

1. **Policy Updates**:
   - Update password policy to require complex, unique passwords
   - Implement regular password rotation schedule
   - Establish incident response procedures for credential stuffing attacks
2. **Training & Awareness**:
   - Conduct security awareness training on credential protection
   - Train users to recognize and report suspicious activities
   - Regular phishing simulation exercises
3. **Proactive Defense**:
   - Regular vulnerability assessments and penetration testing
   - Implement web application firewalls (WAF)
   - Deploy endpoint detection and response (EDR) solutions

8 Conclusion

This investigation confirmed a sophisticated, coordinated multi-user attack campaign characterized by:

- **Early Compromise**: Malware deployment at 05:06:14, indicating initial access before documented connection attempts

- **Account Takeover**: Successful compromise of "charlie" account via internal IP 172.16.0.3
- **Coordinated Infrastructure**: Use of four distinct IP addresses in a pattern targeting multiple users simultaneously
- **Persistent Activity**: Sustained attack over 4+ hours with continuous attempts
- **Data Exfiltration Attempt**: Evidence of file access from external infrastructure

The attack demonstrates characteristics of organized threat actors with medium-to-high sophistication. While immediate containment measures have been implemented, the investigation revealed potential gaps in authentication security and monitoring capabilities that require attention.

8.1 Key Lessons Learned

1. Need for improved detection of credential stuffing campaigns
2. Importance of multi-factor authentication as primary defense
3. Value of comprehensive log correlation across user accounts
4. Necessity of rapid response to early compromise indicators

Annexes

.1 Annexe A: Complete Kibana SIEM Data Export

```
Time,Action,Source IP,Target User,Criticality
04:19:14,Connection attempt,10.0.0.5,david,First attack signal
04:27:14,Connection attempt,172.16.0.3,david,Internal reconnaissance
05:06:14,Malware detected,203.0.113.77,bob,CRITICAL
05:27:14,Connection attempt,203.0.113.77,david,Attacker persistence
05:49:14,Connection attempt,192.168.1.101,charlie,Primary target
06:13:14,Connection attempt,10.0.0.5,charlie,Lateral movement
07:22:14,Connection attempt,192.168.1.101,charlie,Continued targeting
07:36:14,Connection attempt,10.0.0.5,david,Multi-user attack pattern
07:38:14,Connection attempt,172.16.0.3,charlie,Internal pivot point
07:44:14,Connection attempt,203.0.113.77,bob,External C2 communication
07:44:14,Connection attempt,192.168.1.101,bob,Coordinated attack
08:20:14,Connection attempt,192.168.1.101,charlie,Final attempt
08:21:14,Connection attempt,172.16.0.3,david,Attack ongoing
```

.2 Annexe B: IOCs (Indicators of Compromise)

- **IP Addresses**:
  - 203.0.113.77 (External attacker infrastructure)
  - 283.0.113.77 (Data exfiltration)
  - 198.51.100.42 (Initial reconnaissance)

  - 172.16.0.3 (Compromised internal host)
  - 192.168.1.101 (Internal pivot point)
  - 10.0.0.5 (Lateral movement)

- **User Accounts**:
  - charlie (Compromised)
  - david (Targeted)
  - bob (Malware detected)

- **Malware Indicators**:
  - Trojan detected at 07:45:14 from 172.16.0.3
  - Malware detection at 05:06:14 from 203.0.113.77

.3 Annexe D: Incident Communication Email Template

```
TO: Management Team, IT Security Department, CISO
FROM: Security Operations Center (SOC)
DATE: July 5, 2025
SUBJECT: URGENT - Security Incident Notification - IR-2025-007 - Compromised User Acc

Dear Colleagues,

This email serves as an official notification regarding a critical security incident t

INCIDENT SUMMARY:
• Incident ID: IR-2025-007
• Incident Type: Coordinated Multi-User Credential Stuffing Attack with Malware Deploy
• Affected Users: charlie (confirmed compromise), david (targeted), bob (malware detec
• Timeframe: July 3, 2025, 04:19:14 to 08:21:14 UTC
• Severity Level: HIGH

KEY FINDINGS:
1. Credential stuffing campaign targeting multiple user accounts
2. Successful compromise of user "charlie" via internal IP 172.16.0.3
3. Malware (Trojan) detected on bob's account at 05:06:14
4. Evidence of lateral movement within the network
5. Potential data exfiltration attempt detected at 08:42:14

IMMEDIATE ACTIONS TAKEN:
 User accounts charlie, david, and bob have been disabled
 Host at 172.16.0.3 has been isolated for forensic analysis
 Malicious IPs (203.0.113.77, 283.0.113.77, 198.51.100.42) blocked at firewall
 SIEM alerts configured for similar attack patterns

IMPACT ASSESSMENT:
• Data Risk: Files accessed by compromised accounts require investigation
```

```
• Network Risk: Lateral movement detected between internal systems
• Business Impact: Potential unauthorized access to sensitive information

RECOMMENDED NEXT STEPS (Approval Required):
1. Force password reset for all users with suspicious login activity
2. Implement mandatory Multi-Factor Authentication for all accounts
3. Conduct forensic analysis on isolated systems
4. Review and update firewall rules to prevent similar attacks
5. Schedule security awareness training for affected users

INVESTIGATION STATUS:
• Ongoing forensic analysis of compromised systems
• Monitoring for additional suspicious activity
• Complete incident report attached for detailed review

ATTACHMENTS:
• IR-2025-007_Forensic_Report.pdf (Complete investigation report)
• IOC_List_IR-2025-007.csv (Indicators of Compromise)

CONTACT INFORMATION:
• Primary SOC Analyst: Fatima Zahrae Khalil
• SOC Manager: [Manager Name]
• Emergency Contact: SOC Hotline: [Phone Number]

This incident will be reviewed in our weekly security briefing. Please acknowledge rec

Best regards,

Security Operations Center
Future Interns Cybersecurity Program
Email: soc@futureinterns.example.com
Phone: [SOC Phone Number]
```

Usage Notes:

- **Recipients**: Customize based on organizational structure
- **Timing**: Send within 1 hour of incident confirmation
- **Frequency**: Initial notification only - follow-up communications as needed
- **Confidentiality**: Mark as "INTERNAL USE ONLY" for distribution

Communication Protocol:

1. Send initial notification to management and security teams
2. Follow up with technical teams for remediation actions
3. Provide status updates every 4 hours during active response
4. Send final closure notification upon incident resolution

.4 Annexe E: Security Alert Classification Log

Table 9: Security Alert Classification and Prioritization

Time (UTC)	Alert Description	Severity	Priority	Response
05:06:14	Malware detected on bob's session	Critical	P1	Immediate
05:18:14	Successful login - charlie (suspicious IP)	High	P1	Account d
04:23:14	Failed login attempt - charlie	Medium	P3	Monitor ar
07:45:14	Trojan detection - charlie session	High	P1	System iso
08:42:14	Suspicious file access - external IP	High	P2	Data exfilt
04:19:14	Connection attempt - david	Medium	P3	Correlatio
07:44:14	Coordinated attack - multiple users	High	P2	Pattern re
05:49:14	Connection attempt - charlie (post-compromise)	High	P2	Lateral mo

Severity Classification Guidelines:

- **Critical**: Active malware, data exfiltration, system compromise
- **High**: Account compromise, unauthorized access, suspicious privileged activity
- **Medium**: Failed login attempts, reconnaissance activity
- **Low**: Informational alerts, normal suspicious patterns

Priority Levels:

- **P1**: Immediate response required (within 15 minutes)
- **P2**: Response within 1 hour
- **P3**: Response within 4 hours
- **P4**: Response within 24 hours

Table 10: Alert Triage Statistics

Metric	Count	Percentage
Total Alerts Processed	13	100%
Critical Severity Alerts	1	7.7%
High Severity Alerts	5	38.5%
Medium Severity Alerts	7	53.8%
Average Response Time (P1)	22 minutes	-
False Positive Rate	0%	-

SOC Analyst Notes:

```
Analyst: Fatima Zahrae Khalil
Shift: Day Shift (08:00-16:00)
Triage Start: July 3, 2025, 08:30 UTC
Triage Complete: July 3, 2025, 10:45 UTC
Escalations: 2 (to SOC Manager)
Incidents Created: 1 (IR-2025-007)

Key Observations:
1. Pattern indicates coordinated attack rather than isolated incidents
2. Malware detected early in attack chain (05:06:14)
3. Internal IP 172.16.0.3 shows signs of compromise
4. Attack persisted for over 4 hours with continuous attempts
```

References

1. NIST Special Publication 800-61 Rev. 2: Computer Security Incident Handling Guide

2. MITRE ATT&CK Framework: Techniques T1110 (Brute Force), T1078 (Valid Accounts), TA0011 (Command and Control)

3. SANS Institute: Incident Handling Process

4. Kibana SIEM Documentation: Advanced Threat Hunting

5. OWASP: Credential Stuffing Prevention Cheat Sheet