Incident Report – SOC Task 1

Title: Malware Detection Incident Report – Internal Hosts

Prepared By: Komal Ratnaparkhe
Date: 03-Oct-2025

---

1. Executive Summary

On **03-Oct-2025**, the SOC detected multiple malware events across internal hosts using Splunk Enterprise. Alerts included **Ransomware, Trojan, Rootkit, Worm, and Spyware** affecting various users and IP addresses. These events pose a **high risk to data confidentiality, integrity, and availability**, potentially impacting business operations. Immediate containment, remediation, and monitoring measures are recommended to prevent further compromise.

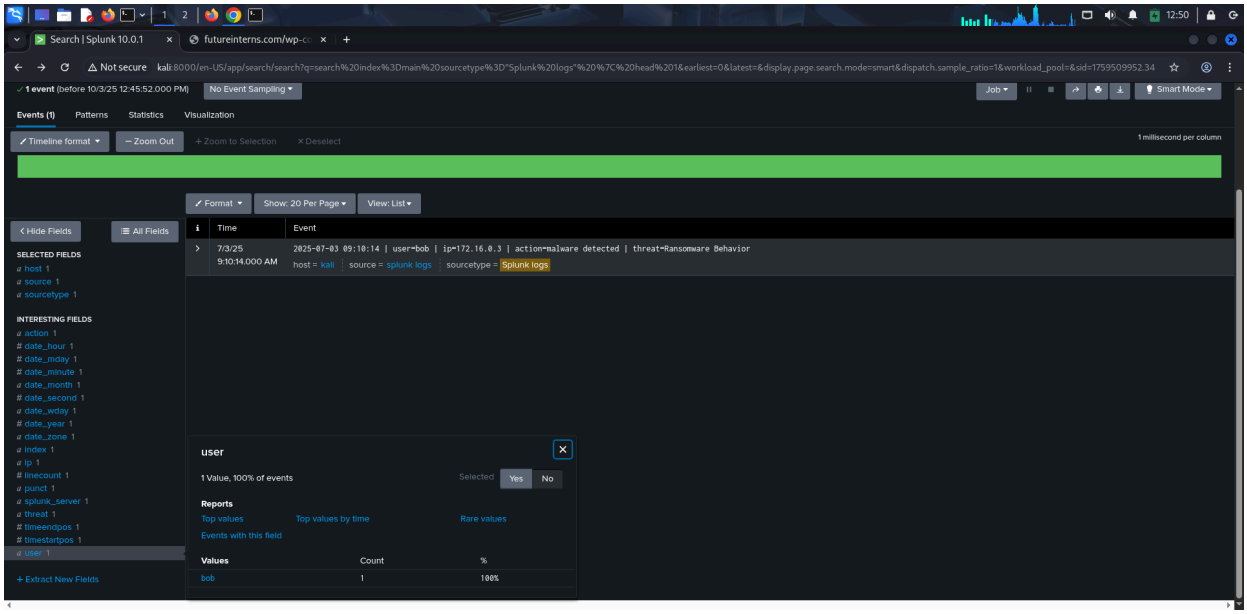
---

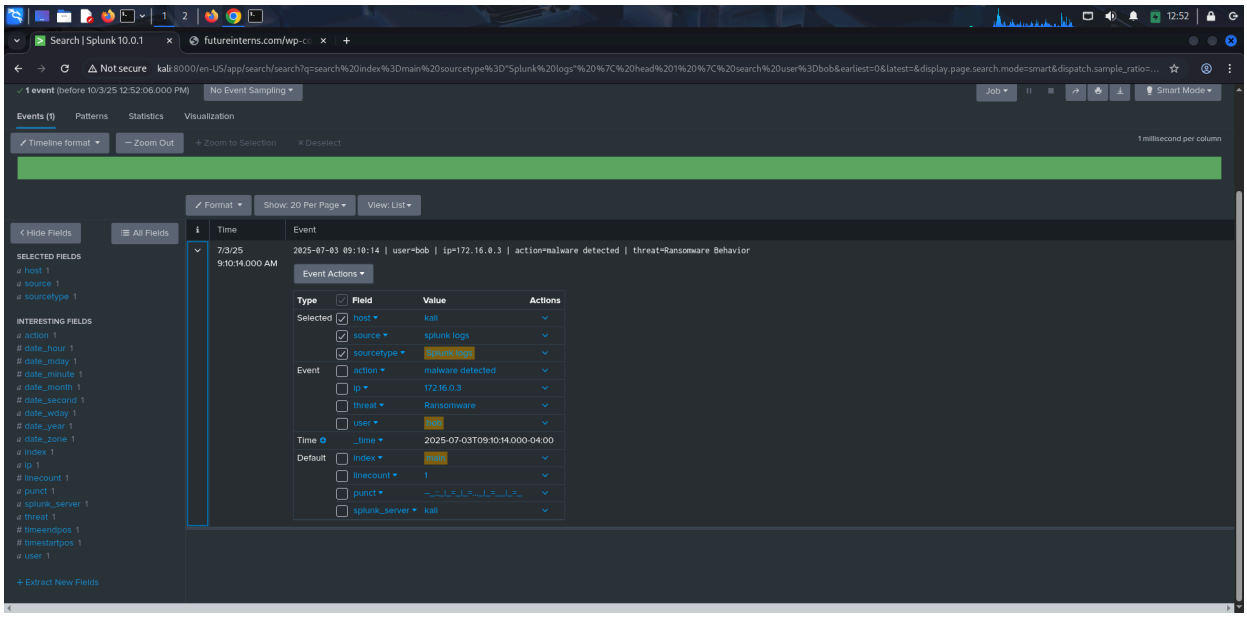
2. Timeline of Events

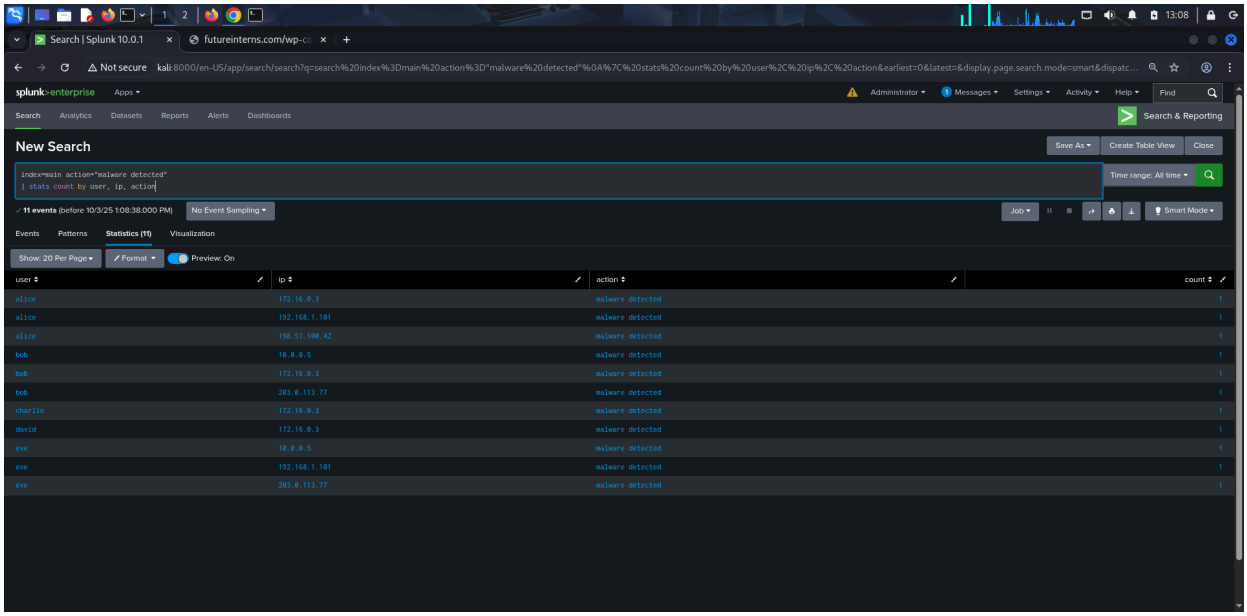
Timestamp	User	IP Address	Action	Threat	Severity	Notes
2025-07-03 09:10:14	bob	172.16.0.3	Malware detected	Ransomware	High	First ransomware alert; critical threat to host.
2025-07-03 07:51:14	eve	10.0.0.5	Malware detected	Rootkit	High	Rootkit detected; host isolation recommended.
2025-07-03 07:45:14	charlie	172.16.0.3	Malware detected	Trojan	High	Trojan detected; could enable remote access.
2025-07-03 05:48:14	bob	10.0.0.5	Malware detected	Trojan	High	Multiple trojan detections; requires remediation.

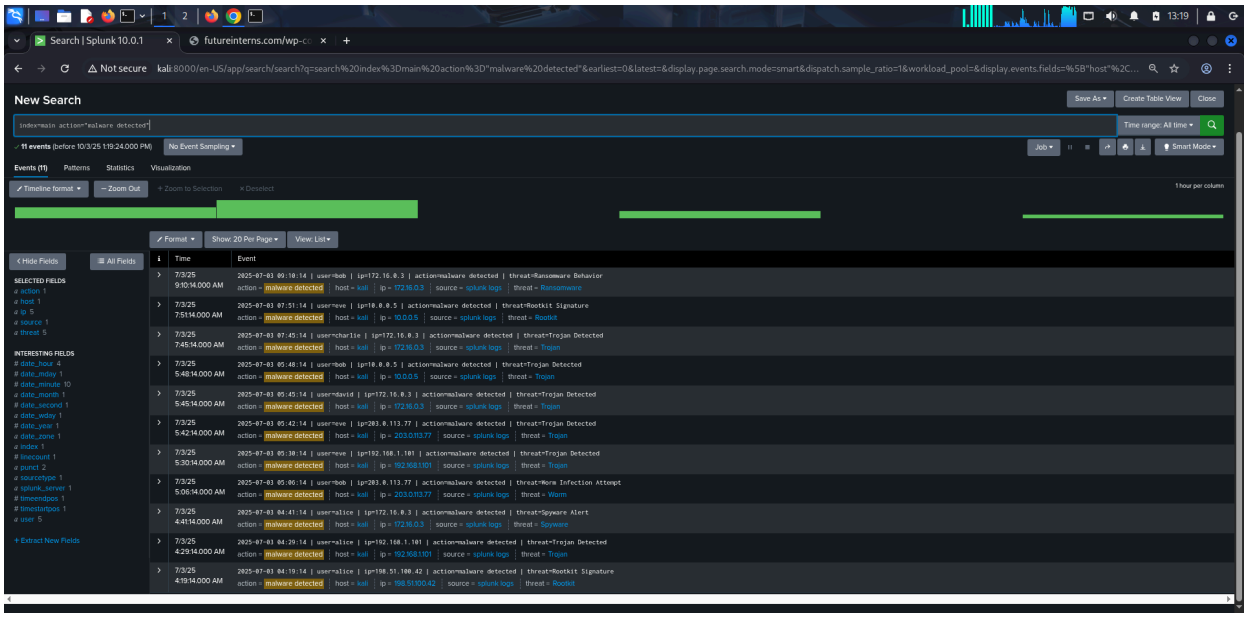
2025-07-03 05:42:14	eric	203.0.113.77	Malware detected	Trojan	High	External IP potentially compromised; monitor traffic.
2025-07-03 05:30:14	eve	192.168.1.101	Malware detected	Trojan	High	Verify antivirus protection.
2025-07-03 05:06:14	bob	203.0.113.77	Malware detected	Worm	High	Worm infection attempt; lateral spread risk.
2025-07-03 04:41:14	alice	172.16.0.3	Malware detected	Spyware	Medium	Spyware alert; possible data exfiltration.
2025-07-03 04:29:14	alice	192.168.1.101	Malware detected	Trojan	High	Verify host isolation.
2025-07-03 04:19:14	alice	198.51.100.42	Malware detected	Rootkit	High	Host may be fully compromised.

Attached Splunk screenshots: next to each event for proof of detection.



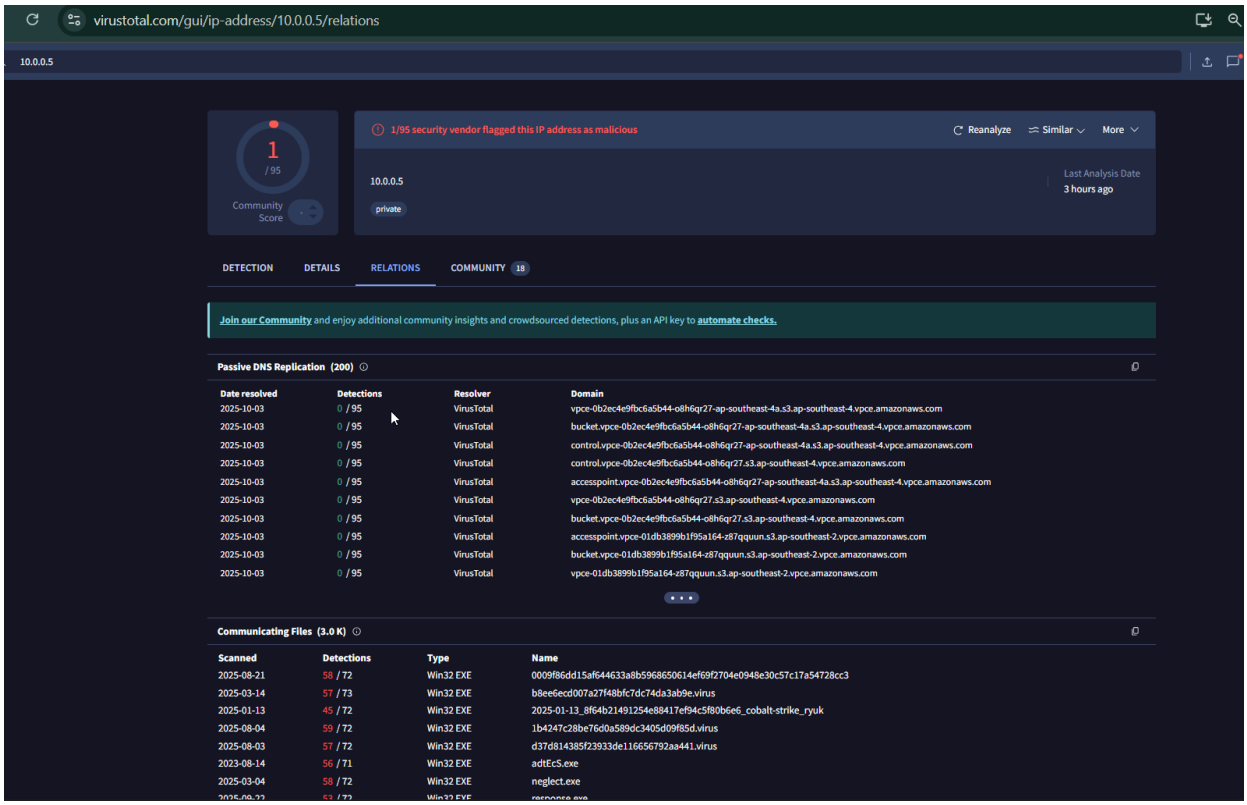

Search | Splunk 10.0.1
futureinterns.com/wp-
Not secure
kali:8000/en-US/app/search/search?q=search%20index%3Dmain%20sourcetype%3D"Splunk%20logs"%20%7C%20head%201%20%7C%20search%20user%3Dbob&earliest=0&latest=&display.page.search.mode=smart&dispatch.sample_ratio=...
1 event (before 10/3/25 12:52:06.000 PM)
No Event Sampling
Job
Smart Mode
Events (1)
Patterns
Statistics
Visualization
Timeline format
Zoom Out
Zoom to Selection
Deselect
1 millisecond per column
Format
Show: 20 Per Page
View: List
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
action 1
date_hour 1
date_mday 1
date_minute 1
date_month 1
date_second 1
date_wday 1
date_year 1
date_zone 1
index 1
ip 1
linecount 1
punct 1
splunk_server 1
threat 1
timeendpos 1
timestartpos 1
user 1
Extract New Fields
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
Event Actions
Type
Field
Value
Actions
Selected
host
kali
source
splunk logs
sourcetype
Splunk logs
Event
action
malware detected
ip
172.16.0.3
threat
Ransomware
user
bob
Time
_time
2025-07-03T09:10:14.000-04:00
Default
index
main
linecount
1
punct
splunk_server
kali

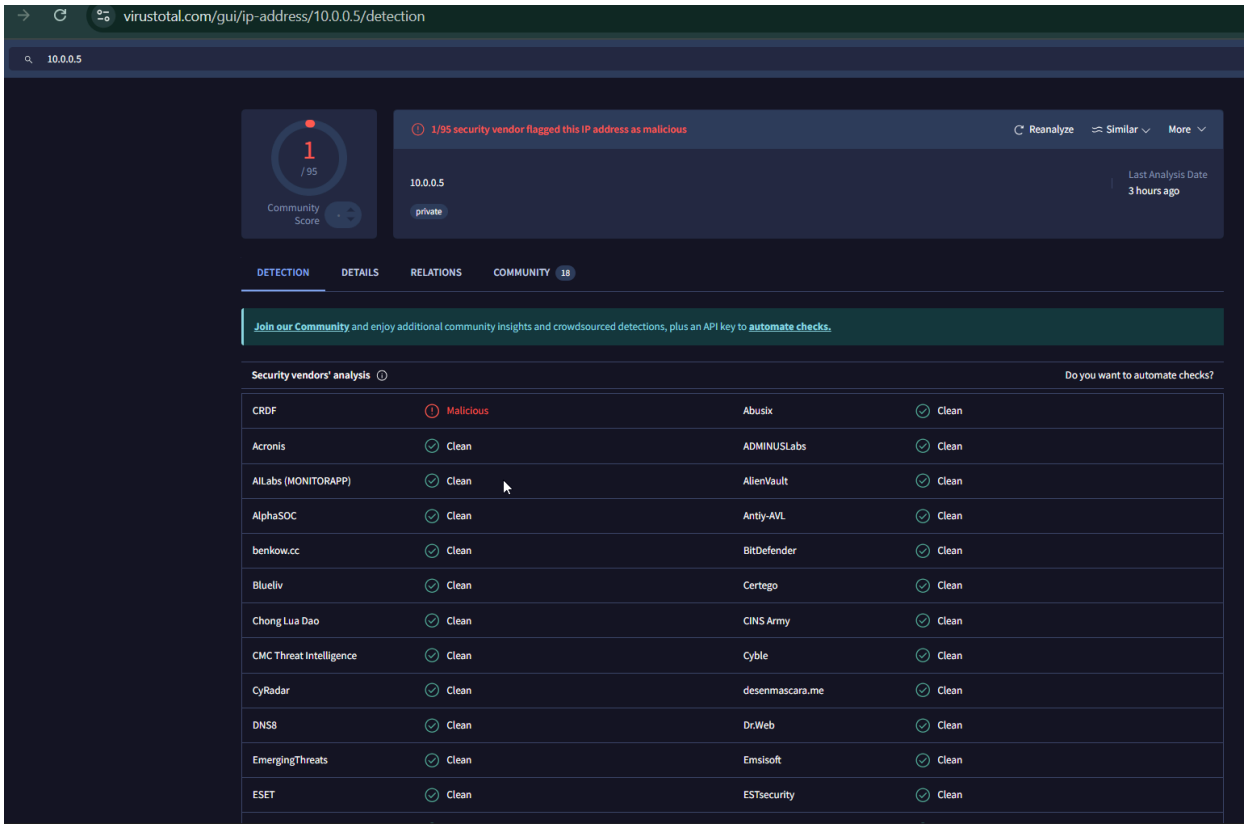

Search | Splunk 10.0.1
futureinterns.com/wp-
Not secure
kali:8000/en-US/app/search/search?q=search%20index%3Dmain%20action%3D"malware%20detected"%0A%7C%20stats%20count%20by%20user%2C%20ip%2C%20action&earliest=0&latest=&display.page.search.mode=smart&dispatc...
splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
index=main action="malware detected"
| stats count by user, ip, action
Time range: All time
11 events (before 10/3/25 1:08:38.000 PM)
No Event Sampling
Job
Smart Mode
Events
Patterns
Statistics (11)
Visualization
Show: 20 Per Page
Format
Preview: On
user
ip
action
count
alice 172.16.0.3 malware detected 1
alice 192.168.1.101 malware detected 1
alice 198.51.100.42 malware detected 1
bob 10.0.0.5 malware detected 1
bob 172.16.0.3 malware detected 1
bob 203.0.113.77 malware detected 1
charlie 172.16.0.3 malware detected 1
david 172.16.0.3 malware detected 1
eve 10.0.0.5 malware detected 1
eve 192.168.1.101 malware detected 1
eve 203.0.113.77 malware detected 1



Threat Intel Verification:

All IP addresses involved in the malware events were verified using VirusTotal, AbuseIPDB, and Talos Intelligence. One internal IP (10.0.0.5) was flagged as potentially malicious by a single security vendor, while all other IPs showed no external threat indicators. This suggests the majority of events originated from internal or non-blacklisted sources. Continuous monitoring and endpoint verification are recommended to detect any lateral movement or future malicious activity.


virustotal.com/gui/ip-address/10.0.0.5/relations
10.0.0.5
1
/ 95
Community Score
1/95 security vendor flagged this IP address as malicious
Reanalyze
Similar
More
10.0.0.5
private
Last Analysis Date
3 hours ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 18
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Passive DNS Replication (200)
Date resolved
Detections
Resolver
Domain
2025-10-03 0 / 95 VirusTotal vpce-0b2ec4e9fbc6a5b44-o8h6qr27-ap-southeast-4a.s3.ap-southeast-4.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal bucket.vpce-0b2ec4e9fbc6a5b44-o8h6qr27-ap-southeast-4a.s3.ap-southeast-4.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal control.vpce-0b2ec4e9fbc6a5b44-o8h6qr27-ap-southeast-4a.s3.ap-southeast-4.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal control.vpce-0b2ec4e9fbc6a5b44-o8h6qr27.s3.ap-southeast-4.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal accesspoint.vpce-0b2ec4e9fbc6a5b44-o8h6qr27-ap-southeast-4a.s3.ap-southeast-4.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal vpce-0b2ec4e9fbc6a5b44-o8h6qr27.s3.ap-southeast-4.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal bucket.vpce-0b2ec4e9fbc6a5b44-o8h6qr27.s3.ap-southeast-4.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal accesspoint.vpce-01db3899b1f95a164-z87qquun.s3.ap-southeast-2.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal bucket.vpce-01db3899b1f95a164-z87qquun.s3.ap-southeast-2.vpce.amazonaws.com
2025-10-03 0 / 95 VirusTotal vpce-01db3899b1f95a164-z87qquun.s3.ap-southeast-2.vpce.amazonaws.com
Communicating Files (3.0 K)
Scanned
Detections
Type
Name
2025-08-21 58 / 72 Win32 EXE 0009f86dd15af644633a8b5968650614ef69f2704e0948e30c57c17a54728cc3
2025-03-14 57 / 73 Win32 EXE b8ee6ecd007a27f48bfc7dc74da3ab9e.virus
2025-01-13 45 / 72 Win32 EXE 2025-01-13_8f64b21491254e88417ef94c5f80b6e6_cobalt-strike_ryuk
2025-08-04 59 / 72 Win32 EXE 1b4247c28be76d0a589dc3405d09f85d.virus
2025-08-03 57 / 72 Win32 EXE d37d814385f23933de116656792aa441.virus
2023-08-14 56 / 71 Win32 EXE adtEcS.exe
2025-03-04 58 / 72 Win32 EXE neglect.exe


virustotal.com/gui/ip-address/10.0.0.5/detection
10.0.0.5
1
/ 95
Community Score
1/95 security vendor flagged this IP address as malicious
Reanalyze
Similar
More
10.0.0.5
private
Last Analysis Date
3 hours ago
DETECTION
DETAILS
RELATIONS
COMMUNITY 18
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Security vendors' analysis
Do you want to automate checks?
CRDF Malicious
Abusix Clean
Acronis Clean
ADMINUSLabs Clean
AILabs (MONITORAPP) Clean
AlienVault Clean
AlphaSOC Clean
Antiy-AVL Clean
benkow.cc Clean
BitDefender Clean
Blueliv Clean
Certego Clean
Chong Lua Dao Clean
CINS Army Clean
CMC Threat Intelligence Clean
Cyble Clean
CyRadar Clean
desenmascara.me Clean
DNS8 Clean
Dr.Web Clean
EmergingThreats Clean
Emsisoft Clean
ESET Clean
ESTsecurity Clean

3. Impact Assessment

- **Confidentiality:** Malware may expose sensitive information on infected hosts.
- **Integrity:** Files may be modified, encrypted, or deleted (ransomware impact).
- **Availability:** Critical systems could be unavailable until remediated.

---

4. Root Cause Hypothesis

- Likely vectors include:
    1. Phishing emails or malicious attachments opened by users.
    2. External devices introducing malware.
    3. Compromised hosts enabling lateral malware spread.

---

5. Containment & Remediation Steps

1. **Isolate infected hosts** immediately from the network.
2. **Block malicious IPs** detected in Splunk alerts.
3. **Run full malware/antivirus scans** on affected hosts.
4. **Reset passwords** for affected users; enforce MFA.
5. **Monitor network traffic** for ongoing anomalies.
6. **Apply security patches** and review endpoint protection policies.

---

6. Next Steps & Lessons Learned

- Update SOC alert rules for Ransomware, Trojan, and Rootkit detection.
- Conduct **user awareness training** for phishing and malware prevention.
- Maintain **regular backups** to mitigate ransomware impact.
- Continuously monitor dashboards and refine alerts for new malware activity.

---

7. Attachments

- Splunk screenshots of each malware detection.
- Malware trend dashboards.
- **Alert Classification Spreadsheet** – Attached to repo.

Alert Classification Spreadsheet Structure

Here's a professional table you can export to CSV:

Timestamp	User	IP Address	Threat	Severity	Detection Tool	Action Taken	Status
2025-07-03 09:10:14	bob	172.16.0.3	Ransomware	High	Splunk	Host isolated	Remediated
2025-07-03 07:51:14	eve	10.0.0.5	Rootkit	High	Splunk	Host isolated	Pending

2025-07-03 07:45:14	charlie	172.16.0.3	Trojan	High	Splunk	Antivirus scan	Remediated
2025-07-03 05:48:14	bob	10.0.0.5	Trojan	High	Splunk	Antivirus scan	Remediated
2025-07-03 05:42:14	eric	203.0.113.77	Trojan	High	Splunk	Monitor traffic	Monitoring
2025-07-03 05:30:14	eve	192.168.1.101	Trojan	High	Splunk	Antivirus scan	Remediated
2025-07-03 05:06:14	bob	203.0.113.77	Worm	High	Splunk	Host isolated	Pending
2025-07-03 04:41:14	alice	172.16.0.3	Spyware	Medium	Splunk	Antivirus scan	Remediated
2025-07-03 04:29:14	alice	192.168.1.101	Trojan	High	Splunk	Host isolated	Remediated
2025-07-03 04:19:14	alice	198.51.100.42	Rootkit	High	Splunk	Host isolated	Pending