Syrian Spyware Incident – Log Analysis Project (2024)

1. Project Title

Spyware Infection Log Analysis Targeting Syrian Users – 2024

2. Abstract

This project presents a realistic, case-study style log analysis of a spyware incident targeting users inside Syria in 2024. A malicious Android application named "PerformanceBooster.apk" was distributed through Telegram channels and untrusted websites and operated as spyware. Using simulated but realistic Sysmon and Network logs, this report demonstrates how a Security Operations Center (SOC) analyst can investigate the incident, identify indicators of compromise (IOCs), and provide remediation recommendations. The project is written to showcase log analysis, threat hunting, and incident investigation skills for SOC and blue team roles.

3. Background and Scenario

In late 2024, multiple users inside Syria reported unusual device behavior after installing a so-called "performance booster" application. The app, shared mainly via Telegram groups and third-party download links, promised to improve phone performance but in reality acted as spyware.

Key malicious behaviors:
- Collecting sensitive data from the device.
- Uploading photos and files to a remote server.
- Tracking basic device information and activity.
- Maintaining persistent communication with a Command-and-Control (C2) server hosted outside Syria.

This project assumes that logs were collected from a Windows 10 host connected to the Android device via a synchronization tool, together with firewall network logs. These logs are then ingested into an ELK Stack (Elasticsearch, Logstash, Kibana) for analysis.

4. Environment and Tools

- Operating System: Windows 10 (host connected to Android device)
- Log Sources:
  - Sysmon logs for process creation and activity.
  - Firewall / network logs for outbound connections and data transfer.
- SIEM Platform: ELK Stack (Elasticsearch, Logstash, Kibana)
- Malicious Application: PerformanceBooster.apk (Android spyware)
- Command-and-Control Server (C2):
  - IP: 185.203.118.55
  - Port: 8082
- Analyst Role: SOC Analyst / Blue Team – log analysis and incident investigation.

5. Log Sources and Sample Entries

5.1 Sysmon – Process Creation (Event ID 1)
Example log entry:

Time: 2024-11-12T14:33:02
EventID: 1
Process Name: sys_perfmon.exe
Parent Process: com.android.settings
User: user1
Hash: e4f2c99ab12d9a12099ffaf83391ddc9

Explanation:
- "sys_perfmon.exe" does not match any known legitimate Windows process.
- The parent process "com.android.settings" suggests an interaction with an Android-related component or management tool.
- The hash value of the executable can be checked against threat intelligence feeds.

5.2 Network Log – Suspicious External Connection
Example log entry:

Time: 2024-11-12T14:33:15
Source IP: 10.0.0.22
Destination IP: 185.203.118.55
Destination Port: 8082
Bytes Sent: 20344
Bytes Received: 1120
User-Agent: android-sync/3.1
Status: Allowed

Explanation:
- The destination IP is a foreign server outside Syria.
- Port 8082 is not a common port for typical Android synchronization traffic.
- The "android-sync/3.1" User-Agent does not match any known legitimate sync client in the environment.

5.3 Data Exfiltration Log – File Upload
Example log entry:

Time: 2024-11-12T14:35:44
Action: File Upload
File: /sdcard/DCIM/Camera/IMG_2211.jpg
Size: 2.1MB
Connection: 185.203.118.55:8082

Explanation:
- Shows direct evidence of exfiltration of a photo from the victim device.
- Repeated events of this type indicate an ongoing data theft operation.

6. Methodology

The investigation follows a structured approach used by SOC analysts:

1) Initial Triage
   - Review alerts related to unusual outbound connections.

- Identify hosts communicating with suspicious IP addresses or ports.

2) Identification of Suspicious Processes
- Search logs for unknown or rare process names.
- Correlate processes with network activity.

3) Network Traffic Analysis
- Filter logs for connections to the suspicious C2 IP and port.
- Measure frequency and volume of communications.

4) Data Exfiltration Detection
- Search for file upload events or unusually large outbound transfers.
- Correlate with known sensitive file paths (e.g., photos, documents).

5) IOC Extraction and Threat Attribution
- Extract IPs, ports, hashes, process names, and user-agent strings.
- Build a list of IOCs for further detection and blocking.

6) Reporting and Recommendations
- Summarize findings.
- Provide remediation steps and long-term security improvements.

7. Detection Queries (Example Kibana / Elasticsearch)

7.1 Detect the Suspicious Process
Query:
process.name: "sys_perfmon.exe"

Purpose:
Find all events where the suspicious process was created or executed.

7.2 Detect C2 Communication
Query:
destination.ip: "185.203.118.55" AND destination.port: 8082

Purpose:
List all outbound connections to the suspected command-and-control server.

7.3 Identify Data Exfiltration Events
Query:
file.operation: "upload" AND destination.ip: "185.203.118.55"

Purpose:
Locate all log entries where files were uploaded to the C2 server.

7.4 Filter by Suspicious User-Agent
Query:
user_agent.original: "android-sync/3.1"

Purpose:
Detect HTTP/HTTPS traffic using the malicious or unknown User-Agent string.

8. Analysis Summary

Based on the logs and queries above, the following behaviors are observed:

- A non-standard process "sys_perfmon.exe" appears on the system and is linked to Android configuration or synchronization activity.
- The host establishes frequent outbound TCP connections to 185.203.118.55 on port 8082, with traffic occurring approximately every 30 seconds.
- Multiple file upload events are recorded, involving images and potentially other files from the device storage.
- Network requests use a suspicious User-Agent string ("android-sync/3.1") that does not belong to any approved or documented application in the organization.

These findings strongly indicate that the device is infected with spyware that is exfiltrating data to an external C2 server.

9. Findings

1) The device has been infected with an Android spyware application disguised as "PerformanceBooster.apk".
2) The spyware establishes a persistent C2 channel with IP 185.203.118.55 over TCP port 8082.
3) Data exfiltration is confirmed through multiple file upload events, including image files from the DCIM/Camera directory.
4) The spyware uses a custom process "sys_perfmon.exe" for execution on the host and a non-standard User-Agent string ("android-sync/3.1").
5) The incident demonstrates a targeted campaign against users inside Syria distributing the malicious APK via Telegram and untrusted sources.

10. Indicators of Compromise (IOCs)

- Malicious Process:
  - sys_perfmon.exe

- File Hash (Example):
  - e4f2c99ab12d9a12099ffaf83391ddc9

- Command-and-Control Server:
  - IP: 185.203.118.55
  - Port: 8082

- Malicious User-Agent:
  - android-sync/3.1

- Malicious APK Name:
  - PerformanceBooster.apk

These IOCs can be fed into SIEM, IDS/IPS, EDR, and firewall systems to detect and block similar activity in the future.

11. Recommendations

1) Immediate Response
- Remove the malicious APK from all affected devices.
- Perform a full factory reset or wipe of compromised Android devices.
- Block outbound traffic to 185.203.118.55 on all network security devices.
- Revoke any exposed credentials that may have been stolen.

2) Hardening and Prevention
- Restrict installation of applications to trusted sources only (e.g., Google Play Store).
- Enforce mobile device management (MDM) policies for users in sensitive roles.
- Deploy endpoint detection and response (EDR) or mobile security solutions to monitor suspicious behavior.
- Configure alerts for unusual outbound traffic patterns, especially to rare ports and foreign IP addresses.

3) User Awareness
- Conduct security awareness training focused on the risks of downloading APKs from Telegram or unknown websites.
- Educate users on recognizing phishing attempts and fake "utility" applications.
- Promote a clear process for reporting suspicious device behavior to the security team.

12. Conclusion

This project demonstrates how log analysis can be used to investigate a realistic spyware incident targeting Syrian users. By carefully examining Sysmon and network logs, a SOC analyst can:

- Identify malicious processes and unusual network behavior.
- Confirm data exfiltration and active command-and-control communication.
- Extract actionable Indicators of Compromise (IOCs).
- Recommend effective remediation and long-term prevention measures.

The techniques and methodology shown in this report are directly applicable to real-world SOC, blue team, and incident response work. This project can be used as a portfolio piece to showcase log analysis, threat hunting, and incident investigation skills, especially in environments where mobile devices and regional threats play a significant role.

Appendix A – Compact Sample Logs

Sysmon – Process Creation:
2024-11-12T14:33:02 | EventID=1 | Process=sys_perfmon.exe | Parent=com.android.settings | User=user1

Network – C2 Connection:
2024-11-12T14:33:15 | Src=10.0.0.22 | Dst=185.203.118.55 | Port=8082 | UA=android-sync/3.1 | BytesSent=20344

Data Exfiltration:
2024-11-12T14:35:44 | Action=Upload | File=/sdcard/DCIM/Camera/IMG_2211.jpg | Size=2.1MB | Dst=185.203.118.55:8082