INDEX

- Introduction
- Device Data
- Analysis Result
- Conclusions
- MITRE ATT&CK Analysis
- Useful Contacts
- Connections Relevant for Analysis
- Application Behavior (App Behavior)
- TLS Fingerprints Analysis (JA3/JA4)
- File Transfer Analysis
- TLS Certificate Characteristics
- Forensic Analysis - Alternative Hypotheses
- Uncategorized Communications
- Whitelisted communications

Introduction

This report aims to provide information on the analysis of the scanned device. During the analysis, various aspects are examined, such as network communications, protocols used, suspicious connections, secure certificates, and many other indicators of compromise.

Through the analysis of data and evidence collected, signals of compromise, vulnerabilities, rules are identified in order to evaluate whether the device's data capture shows signs of compromise or harmful activities that could put the user's security at risk. The ultimate goal is to provide a clear and simple assessment that helps to understand whether the device is secure or compromised and if it requires further actions or risk mitigation.

MITRE ATT&CK Analysis Methodology

This forensic analysis uses both MITRE ATT&CK Enterprise and MITRE ATT&CK Mobile matrices (v18.1). Any discrepancies in severity levels between the two matrices are normal and expected: the Enterprise matrix is designed for threats targeting traditional

IT infrastructure (servers, workstations, corporate networks), while the Mobile matrix is specifically calibrated for mobile devices (Android/iOS) and spyware/stalkerware. The same attack technique may have different impacts and frequencies in each context, justifying different risk classifications.

DEVICE ACQUISITION DATA
Device name: Meeting
Device description:
Report generated on 17/01/2026 - 00:06:48
Capture duration: 556.507508 seconds
Number of packets: 29125
Capture SHA1: 8de92e5bead6663d2798ab5a536cf10d1f77d653

Analysis Result

Detected 14 high-priority indicators requiring in-depth analysis.

Conclusions

Quantitative Summary

Analysis identified: 14 high-priority indicators (breakdown: 11 CRITICAL + 3 HIGH = 14 total), none at medium priority, and none at low priority.

Forensic Assessment (OIHL Framework)

Risk Level: CRITICAL

Recommended Action: Immediate Isolation

Isolate device immediately and preserve evidence for forensic analysis.

Summary: Critical threat detected: 11 critical findings, active C2 communication suspected.

Technical Interpretation

High-Priority Indicators Detected

The analysis identified high-priority indicators that are consistent with patterns observed in compromised devices. These indicators have high confidence based on threat intelligence correlation and behavioral analysis. Immediate review is recommended.

Recommended actions: preserve evidence, consult forensic specialist, consider device isolation pending investigation.

High-Priority Indicators Detected

The following specific IP addresses and domains triggered high-priority alerts:

Type	IP Address	Domain	Technique	Confidence
Forensic	**45.207.200.251**	app.nfuenglish2025.com	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	62%
Forensic	**45.207.207.168**	app.nfuenglish2025.com	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	48%
Forensic	**app.nfuenglish2025.com**	-	T1041, T1029, T1071 Exfiltration Over C2 Channel, Scheduled Transfer, Application Layer Protocol	42%
Forensic	**101.32.207.8**	101.32.207.8	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	42%
Forensic	**43.159.143.39**	43.159.143.39	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	42%
Forensic	**43.157.1.82**	43.157.1.82	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	42%
Forensic	**43.157.184.190**	43.157.184.190	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	42%
Forensic	**43.160.255.143**	43.160.255.143		42%

Type	IP Address	Domain	Technique	Confidence
			T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	
Forensic	**154.90.54.222**	154.90.54.222	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	42%
Forensic	**43.159.99.24**	ws.rc8820.com	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	34%
Forensic	**101.32.207.8:8080**	-	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	31%
Forensic	**43.159.143.39:8080**	-	T1041, T1071 Exfiltration Over C2 Channel, Application Layer Protocol	31%
Forensic	**app.nfuenglish2025.com**	app.nfuenglish2025.com	T1417.001 Keylogging	60%
Forensic	**multiple**	multiple	T1637.001 Domain Generation Algorithms	55%

MITRE ATT&CK Analysis

Framework Version: ATT&CK v18.1 (November 2025)

ATT&CK Enterprise Techniques Detected

Total unique techniques: 3

T1041	Exfiltration Over C2 Channel	12	CRITICAL
T1071	Application Layer Protocol	12	HIGH

T1029	Scheduled Transfer	1	HIGH

Cyber Kill Chain Progression

Actions
12
IPs

Complete Kill Chain Analysis

All monitored IPs with their attack progression scores:

IP Address	Domain	Score	Furthest Phase
app.nfuenglish2025.com	Unknown	100.0%	Actions on Objectives
101.32.207.8	101.32.207.8	100.0%	Actions on Objectives
43.159.99.24	ws.rc8820.com	100.0%	Actions on Objectives
43.159.143.39	43.159.143.39	100.0%	Actions on Objectives
43.157.1.82	43.157.1.82	100.0%	Actions on Objectives
43.157.184.190	43.157.184.190	100.0%	Actions on Objectives
43.160.255.143	43.160.255.143	100.0%	Actions on Objectives
154.90.54.222	154.90.54.222	100.0%	Actions on Objectives
45.207.207.168	app.nfuenglish2025.com	100.0%	Actions on Objectives
45.207.200.251	app.nfuenglish2025.com	100.0%	Actions on Objectives
101.32.207.8:8080	Unknown	100.0%	Actions on Objectives
43.159.143.39:8080	Unknown	100.0%	Actions on Objectives

Critical Findings with ATT&CK Mapping

45.207.200.251 CRITICAL

Confidence: 61.6% (95% CI: 51.2% - 70.0%) | Kill Chain: Actions on Objectives

Techniques: T1041, T1071

⚡ Recommended Action: Isolate - Active C2/exfiltration detected in kill chain phase: Actions on Objectives

---

45.207.207.168 CRITICAL

Confidence: 47.9% (95% CI: 37.5% - 56.7%) | Kill Chain: Actions on Objectives

Techniques: T1041, T1071

⚡ Recommended Action: Isolate - Active C2/exfiltration detected in kill chain phase: Actions on Objectives

---

app.nfuenglish2025.com CRITICAL

Confidence: 42.2% (95% CI: 32.8% - 51.8%) | Kill Chain: Actions on Objectives

Techniques: T1041, T1029, T1071

⚡ Recommended Action: Isolate - Active C2/exfiltration detected in kill chain phase: Actions on Objectives

---

101.32.207.8 CRITICAL

Confidence: 42.1% (95% CI: 32.8% - 51.8%) | Kill Chain: Actions on Objectives

Techniques: T1041, T1071

⚡ Recommended Action: Isolate - Active C2/exfiltration detected in kill chain phase: Actions on Objectives

---

43.159.143.39 CRITICAL

Confidence: 42.1% (95% CI: 32.8% - 51.8%) | Kill Chain: Actions on Objectives

Techniques: T1041, T1071

⚡ Recommended Action: Isolate - Active C2/exfiltration detected in kill chain phase: Actions on Objectives

STIX 2.1 Export Available

Threat intelligence bundle generated for sharing:

- 14 Indicators (IOC)
- 27 Attack Patterns (MITRE ATT&CK)

Export file: stix_bundle.json - Compatible with MISP, OpenCTI and other TIP platforms

Chain of Custody

Evidence Items: 3 | Integrity: Verified

SHA256 hashes and custody logs available in evidence_chain/ directory

MITRE ATT&CK Mobile Analysis

Mobile Threat Summary

2	1	2	0
Mobile Techniques	PCAP Verifiable	Evidence Items	High Confidence

T1417.001	Keylogging	1	Indirect	
T1637.001	Domain Generation Algorithms	1	⚠ Heuristic	⚠

Evidence Details (IP/Domain)

Technique	Target IP	Target Domain	Confidence	Evidence
T1417.001 Keylogging	app.nfuenglish2025.com	app.nfuenglish2025.com	60%	Detected 14 small POST requests (avg 28 bytes, interval 22.0s) to app.nfuenglish
T1637.001 Domain Generation Algorithms	-	app.nfuenglish2025.com	55%	Detected 3 potential DGA domains (avg entropy: 3.52)

⚖ Forensic Risk Assessment

Warning: The following techniques have limited PCAP visibility. Additional device-level evidence is required for declarative conclusions:

MEDIUM RISK - Declare with caution

- T1637.001 (Domain Generation Algorithms): observability MEDIUM

Recommendation: For techniques with limited network observability, include in reports only with supporting evidence (device logs, app analysis, user interviews).

PCAP Observability Classification

Indirect

1

Inferable from network patterns

T1417.001

⚠ Heuristic

1

Requires behavioral analysis

T1637.001

Mobile Tactics Observed

Mobile tactics identified via network traffic analysis:

Command and Control | Credential Access

Useful Contacts

Contact information to obtain further assistance or resources:

info@securepath.biz

DETAILED TECHNICAL DATA

The following sections contain raw technical data for in-depth analysis. The alerts shown (MODERATE, LOW) indicate individual anomalies and do NOT represent the final verdict, which is exclusively determined by the Analysis Result section above.

Connections Relevant for Analysis

Each suspicious connection has been correlated with the responsible application using TLS SNI, DNS, temporal correlation and ASN.

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑ up ↓ down)	REASON
Unknown	0%	HIGH	101.32.207.8:8080	TCP http,websocket	↑ 37.7 KB ↓ 16.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 101.32.207.8:8080

HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05

⚠ Vulnerability/Threat: 120 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑ up ↓ down)	REASON
Unknown	0%	HIGH	101.32.207.8:8080	TCP http	↑ 37.7 KB ↓ 16.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 101.32.207.8:8080

HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
⚠ Vulnerability/Threat: 120 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	0%	HIGH	154.90.54.222:8080	TCP http	↑ 3.6 KB ↓ 1.2 KB	No TLS SNI, DNS, or temporal correlation evidence for 154.90.54.222:8080
HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05 ⚠ Vulnerability/Threat: 17 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	0%	HIGH	43.157.1.82:8080	TCP http	↑ 3.6 KB ↓ 1.2 KB	No TLS SNI, DNS, or temporal correlation evidence for 43.157.1.82:8080
HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05 ⚠ Vulnerability/Threat: 17 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	0%	HIGH	43.157.184.190:8080	TCP http	↑ 4.2 KB ↓ 1.2 KB	No TLS SNI, DNS, or temporal correlation evidence for 43.157.184.190:8080
HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05 ⚠ Vulnerability/Threat: 17 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	0%	HIGH	43.159.143.39:8080	TCP http	↑ 14.4 KB ↓ 8.9 KB	No TLS SNI, DNS, or temporal correlation evidence for 43.159.143.39:8080
HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05						

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
⚠ Vulnerability/Threat: 40 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	0%	HIGH	43.159.143.39:8080	TCP http,websocket	↑ 14.4 KB ↓ 8.9 KB	No TLS SNI, DNS, or temporal correlation evidence for 43.159.143.39:8080
HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05 ⚠ Vulnerability/Threat: 40 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	0%	HIGH	43.160.255.143:8080	TCP http	↑ 4.0 KB ↓ 1.2 KB	No TLS SNI, DNS, or temporal correlation evidence for 43.160.255.143:8080
HIGH 4x Alerts: BEHAV-03, BEHAV-08, PROTO-02, PROTO-05 ⚠ Vulnerability/Threat: 17 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	33%	HIGH	app.nfuenglish2025.com 45.207.207.168:80	TCP http	↑ 1.2 KB ↓ 1.9 KB	No TLS SNI, DNS, or temporal correlation evidence for 45.207.207.168:80 DNS: app.nfuenglish2025.com, PORT: 80
HIGH 3x Alerts: ACT-02, BEHAV-10, PROTO-03 ⚠ Vulnerability/Threat: The domain name app.nfuenglish2025.com is quite new. Even this is not malicious by itself, its quite common for attackers to set up new infrastructure for each attack campaign which can lead to the use of recently registered domain names.						
Unknown	33%	HIGH	app.nfuenglish2025.com 45.207.207.168:80	TCP http	↑ 1.2 KB ↓ 1.9 KB	No TLS SNI, DNS, or temporal correlation evidence for 45.207.207.168:80 DNS: app.nfuenglish2025.com, PORT: 80

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
HIGH 3x Alerts: ACT-02, BEHAV-10, PROTO-03 ⚠ Vulnerability/Threat: The domain name app.nfuenglish2025.com is quite new. Even this is not malicious by itself, its quite common for attackers to set up new infrastructure for each attack campaign which can lead to the use of recently registered domain names.						
Unknown	33%	HIGH	app.nfuenglish2025.com 45.207.200.251:80	TCP http	↑ 6.7 KB ↓ 10.1 KB	No TLS SNI, DNS, or temporal correlation evidence for 45.207.200.251:80 DNS: app.nfuenglish2025.com, PORT: 80
HIGH 3x Alerts: ACT-02, BEHAV-10, PROTO-03 ⚠ Vulnerability/Threat: The domain name app.nfuenglish2025.com is quite new. Even this is not malicious by itself, its quite common for attackers to set up new infrastructure for each attack campaign which can lead to the use of recently registered domain names.						
Unknown	33%	HIGH	app.nfuenglish2025.com 45.207.200.251:80	TCP http	↑ 6.7 KB ↓ 10.1 KB	No TLS SNI, DNS, or temporal correlation evidence for 45.207.200.251:80 DNS: app.nfuenglish2025.com, PORT: 80
HIGH 3x Alerts: ACT-02, BEHAV-10, PROTO-03 ⚠ Vulnerability/Threat: The domain name app.nfuenglish2025.com is quite new. Even this is not malicious by itself, its quite common for attackers to set up new infrastructure for each attack campaign which can lead to the use of recently registered domain names.						
Unknown	28%	HIGH	ws.rc8820.com 43.159.99.24:8080	TCP http	↑ 2.4 KB ↓ 1.4 KB	No TLS SNI, DNS, or temporal correlation evidence for 43.159.99.24:8080 DNS: ws.rc8820.com
HIGH 2x Alerts: BEHAV-03, BEHAV-08						

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
⚠ Vulnerability/Threat: 16 small packets uploaded. This pattern is consistent with real-time location tracking, SMS interception, or call log exfiltration. Stalkerware apps typically send small frequent updates.						
Unknown	33%	MODERATE	nfc.nfu829.com 43.153.232.152:443	TCP ssl	↑ 7.5 KB ↓ 9.7 MB	No TLS SNI, DNS, or temporal correlation evidence for 43.153.232.152:443 DNS: nfc.nfu829.com, PORT: 443
MODERATE ACT-02 ⚠ Vulnerability/Threat: The domain name nfc.nfu829.com is quite new. Even this is not malicious by itself, its quite common for attackers to set up new infrastructure for each attack campaign which can lead to the use of recently registered domain names.						
Unknown	28%	MODERATE	ws.rc8820.com 43.159.98.31:8080	TCP http	↑ 180 B ↓ 92 B	No TLS SNI, DNS, or temporal correlation evidence for 43.159.98.31:8080 DNS: ws.rc8820.com
MODERATE 2x Alerts: ACT-02, PROTO-02 ⚠ Vulnerability/Threat: The domain name ws.rc8820.com is quite new. Even this is not malicious by itself, its quite common for attackers to set up new infrastructure for each attack campaign which can lead to the use of recently registered domain names.						
Unknown	50%	MODERATE	edgedl.me.gvt1.com 34.104.35.123:80	TCP http	↑ 3.7 KB ↓ 5.7 MB	No TLS/DNS evidence for 34.104.35.123:80 on Infrastructure provider: google-cloud-platform DNS: edgedl.me.gvt1.com, ASN: Infrastructure provider: google-cloud-platform, PORT: 80
MODERATE 12x Alerts: BEHAV-08, FILE-06 ⚠ Vulnerability/Threat: File '' (4513.6KB) uploaded to 34.104.35.123 via Unknown						
Unknown	50%	MODERATE	edgedl.me.gvt1.com 34.104.35.123:443	TCP tls	↑ 0 B ↓ 574 B	No TLS/DNS evidence for 34.104.35.123:443 on Infrastructure provider: google-cloud-platform DNS: edgedl.me.gvt1.com, ASN: Infrastructure provider: google-cloud-platform, PORT: 443

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON

MODERATE 12x Alerts: BEHAV-08, FILE-06

⚠ Vulnerability/Threat: File '' (4513.6KB) uploaded to 34.104.35.123 via Unknown

Application Behavior (App Behavior)

This section shows the attribution of network flows to the responsible mobile applications, with an explanation of the evidence used for identification.

Unknown ⚠ - Suspicious (15 flows)

Total flows: 24 | Average confidence: 33%

Protocols	Domains	ASN	IP Addresses
tcp	app.nfuenglish2025.com de0mpg.cdn-settings.appsflyersdk.com edgedl.me.gvt1.com events.swishapps.ai nfc.nfu829.com pro-client-config.swishapps.ai sdk-01.moengage.com vzwappprofile.vzw.com ws.rc8820.com	--	10.10.2.101 101.32.207.8 13.32.104.125 143.204.130.117 154.90.54.222 173.194.208.94 23.206.56.116 34.104.35.123 34.150.232.69 34.8.241.29

Detailed Flows (Forensic View) - Grouped by Domain

⚠ IP/ASN (10 flows)

Status	Proto	Destination	Bytes	Evidence
⚠	tcp:8080	101.32.207.8	↑37.7KB ↓16.7KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	101.32.207.8	↑37.7KB ↓16.7KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	154.90.54.222	↑3.6KB ↓1.2KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	43.157.1.82	↑3.6KB ↓1.2KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	43.157.184.190	↑4.2KB ↓1.2KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	43.159.143.39	↑14.4KB ↓8.9KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	43.159.143.39	↑14.4KB ↓8.9KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	43.160.255.143	↑4.0KB ↓1.2KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:37304	10.10.2.101	↑827B ↓66B	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	173.194.208.94	↑152B ↓184B	No TLS/DNS evidence for 173.194.208.94:4...

⚠ nfuenglish2025.com (4 flows)

Status	Proto	Destination	Bytes	Evidence
⚠	tcp:80	app.nfuenglish2025.com	↑1.2KB ↓1.9KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:80	app.nfuenglish2025.com	↑1.2KB ↓1.9KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:80	app.nfuenglish2025.com	↑6.7KB ↓10.1KB	No TLS SNI, DNS, or temporal correlation...

Status	Proto	Destination	Bytes	Evidence
⚠	tcp:80	app.nfuenglish2025.com	↑6.7KB ↓10.1KB	No TLS SNI, DNS, or temporal correlation...

⚠ rc8820.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
⚠	tcp:8080	ws.rc8820.com	↑2.4KB ↓1.4KB	No TLS SNI, DNS, or temporal correlation...
⚠	tcp:8080	ws.rc8820.com	↑180B ↓92B	No TLS SNI, DNS, or temporal correlation...

⚠ nfu829.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
⚠	tcp:443	nfc.nfu829.com	↑7.5KB ↓9.71MB	No TLS SNI, DNS, or temporal correlation...

✓ gvt1.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:80	edgedl.me.gvt1.com	↑3.7KB ↓5.73MB	No TLS/DNS evidence for 34.104.35.123:80...
✓	tcp:443	edgedl.me.gvt1.com	↑0 ↓574B	No TLS/DNS evidence for 34.104.35.123:44...

✓ swishapps.ai (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	events.swishapps.ai	↑6.3KB ↓5.8KB	No TLS/DNS evidence for 34.150.232.69:44...

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pro-client-config.swishapps.ai	↑908B ↓5.2KB	No TLS/DNS evidence for 34.8.241.29:443 ...

✓ appsflyersdk.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	de0mpg.cdn-settings.appsflyersdk.com	↑921B ↓5.4KB	No TLS/DNS evidence for 143.204.130.117:...

✓ moengage.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sdk-01.moengage.com	↑2.9KB ↓5.6KB	No TLS/DNS evidence for 13.32.104.125:44...

✓ vzw.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	vzwappprofile.vzw.com	↑1.2KB ↓5.5KB	No TLS SNI, DNS, or temporal correlation...

Google ✓ - Legitimate

Total flows: 36 | Average confidence: 92%

Protocols	Domains	ASN	IP Addresses
tcp, udp	accounts.google.com android-safebrowsing.google.com	--	10.10.2.1 141.207.227.233

Protocols	Domains	ASN	IP Addresses
	clients4.google.com digitalassetlinks.googleapis.com firebase-settings.crashlytics.com inbox.google.com infinitedata-pa.googleapis.com mail.google.com play-fe.googleapis.com play.google.com		142.250.113.139 142.250.113.17 142.250.113.94 142.250.113.95 142.250.114.105 142.250.114.94 142.250.114.95 142.250.115.95

Detailed Flows (Forensic View)

Timestamp	Status	Proto	Destination	Bytes	Evidence
2025-10-0300:51:33	✓ Legitimate	udp/dns: 53	10.10.2.1	↑2.5KB ↓7.4KB	UDP flow inherited context from TLS SNI: update.googleapi...
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	142.251.186.94	↑1.6KB ↓7.0KB	TLS SNI direct match: connectivitycheck.gstatic.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	accounts.google.com (142.251.186.84)	↑5.9KB ↓10.4KB	DNS correlation: accounts.google.com → 142.251.186.84
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	android-safebrowsing.google.com (142.251.116.91)	↑9.8KB ↓16.6KB	TLS SNI direct match: android-safebrowsing.google.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	android-safebrowsing.google.com (142.251.116.91)	↑9.8KB ↓16.6KB	TLS SNI direct match: android-safebrowsing.google.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	clients4.google.com (142.251.186.102)	↑14.7KB ↓20.0KB	TLS SNI direct match: android.apis.google.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	clients4.google.com (142.251.186.102)	↑14.7KB ↓20.0KB	TLS SNI direct match: android.apis.google.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	digitalassetlinks.googleapis.com (192.178.220.95)	↑9.2KB ↓16.7KB	TLS SNI direct match: taskassist-pa.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	digitalassetlinks.googleapis.com (192.178.220.95)	↑9.2KB ↓16.7KB	TLS SNI direct match: taskassist-pa.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/tls: 443	firebase-settings.crashlytics.com (142.250.113.94)	↑24.9KB ↓28.5KB	TLS SNI direct match: update.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	firebase-settings.crashlytics.com (142.250.113.94)	↑24.9KB ↓28.5KB	TLS SNI direct match: update.googleapis.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	firebase-settings.crashlytics.com (142.250.113.94)	↑24.9KB ↓28.5KB	TLS SNI direct match: update.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	inbox.google.com (142.250.113.17)	↑2.93MB ↓119.2KB	TLS SNI direct match: inbox.google.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	infinitedata-pa.googleapis.com (142.250.113.95)	↑8.2KB ↓21.9KB	TLS SNI direct match: peoplestack-pa.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	infinitedata-pa.googleapis.com (142.250.115.95)	↑12.2KB ↓20.3KB	TLS SNI direct match: firebaselogging.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/tls: 443	infinitedata-pa.googleapis.com (142.250.138.95)	↑63B ↓73B	DNS correlation: android.googleapis.com → 142.250.138.95
2025-10-0300:51:33	✓ Legitimate	tcp/tls: 443	infinitedata-pa.googleapis.com (142.251.116.95)	↑42.6KB ↓224.8KB	TLS SNI direct match: peoplestack-pa.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	infinitedata-pa.googleapis.com (142.250.114.95)	↑7.6KB ↓12.1KB	TLS SNI direct match: firebaseremoteconfig.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	infinitedata-pa.googleapis.com (142.251.116.95)	↑42.6KB ↓224.8KB	TLS SNI direct match: peoplestack-pa.googleapis.com
2025-10-0300:51:33					

Timestamp	Status	Proto	Destination	Bytes	Evidence
	✓ Legitimate	udp/ quic,ssl: 443	infinitedata-pa.googleapis.com (142.250.115.95)	↑12.2KB ↓20.3KB	TLS SNI direct match: firebaselogging.googleapis.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	infinitedata-pa.googleapis.com (142.251.116.95)	↑42.6KB ↓224.8KB	TLS SNI direct match: peoplestack-pa.googleapis.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	infinitedata-pa.googleapis.com (173.194.208.95)	↑54.0KB ↓53.0KB	DNS correlation: android.googleapis.com → 173.194.208.95
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	mail.google.com (142.251.186.83)	↑6.6KB ↓13.6KB	TLS SNI direct match: mail.google.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	mail.google.com (142.251.186.17)	↑3.1KB ↓12.5KB	TLS SNI direct match: mail.google.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	play-fe.googleapis.com (142.250.113.139)	↑11.0KB ↓8.0KB	TLS SNI direct match: clients4.google.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	play.google.com (142.250.138.139)	↑862B ↓11.1KB	TLS SNI direct match: play.google.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	play.google.com (142.250.138.102)	↑12.8KB ↓15.6KB	DNS correlation: play.google.com → 142.250.138.102
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	play.googleapis.com (216.239.32.223)	↑95.6KB ↓38.4KB	TLS SNI direct match: play.googleapis.com
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl: 443	play.googleapis.com (216.239.32.223)	↑95.6KB ↓38.4KB	TLS SNI direct match: play.googleapis.com
2025-10-0300:51:33	✓ Legitimate	tcp/ssl: 443	update.googleapis.com (142.250.114.94)	↑19.4KB ↓21.8KB	TLS SNI direct match: update.googleapis.com
2025-10-0300:51:33	✓ Legitimate		update.googleapis.com (142.250.114.94)	↑19.4KB ↓21.8KB	TLS SNI direct match: update.googleapis.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
		udp/quic,ssl:443			
2025-10-0300:51:33	✓ Legitimate	udp/ipsec:500	wo.vzwwo.com (141.207.227.233)	↑1.7KB ↓1.7KB	UDP flow inherited context from TLS SNI: update.googleapi...
2025-10-0300:51:33	✓ Legitimate	udp/ipsec:4500	wo.vzwwo.com (141.207.227.233)	↑13.8KB ↓9.3KB	UDP flow inherited context from TLS SNI: update.googleapi...
2025-10-0300:51:33	✓ Legitimate	udp/quic,ssl:443	www.google.com (142.251.116.99)	↑5.1KB ↓5.2KB	DNS correlation: www.google.com → 142.251.116.99
2025-10-0300:51:33	✓ Legitimate	tcp/ssl:443	www.google.com (142.250.114.105)	↑7.1KB ↓13.8KB	TLS SNI direct match: www.google.com
2025-10-0300:51:33	✓ Legitimate	udp/quic,ssl:443	www.google.com (142.250.114.105)	↑7.1KB ↓13.8KB	TLS SNI direct match: www.google.com

Facebook ✓ - Legitimate

Total flows: 2 | Average confidence: 100%

Protocols	Domains	ASN	IP Addresses
tcp	www.facebook.com	--	157.240.24.35

Detailed Flows (Forensic View)

Timestamp	Status	Proto	Destination	Bytes	Evidence
2025-10-0300:51:33	✓ Legitimate	tcp/tls:443		↑1.1KB ↓5.5KB	TLS SNI direct match: www.facebook.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
			www.facebook.com (157.240.24.35)		
2025-10-0300:51:33	✓ Legitimate	tcp/ssl:443	www.facebook.com (157.240.24.35)	↑1.1KB ↓5.5KB	TLS SNI direct match: www.facebook.com

Twitter ✓ - Legitimate

Total flows: 1 | Average confidence: 66%

Protocols	Domains	ASN	IP Addresses
udp	lh3.googleusercontent.com	--	142.250.114.132

Detailed Flows (Forensic View)

Timestamp	Status	Proto	Destination	Bytes	Evidence
2025-10-0300:51:33	✓ Legitimate	udp/ quic,ssl:443	lh3.googleusercontent.com (142.250.114.132)	↑12.7KB ↓159.6KB	DNS correlation: mail-attachment.googleusercontent.com → ...

Attribution Methodology

Application attribution is based on multi-level correlation that includes:

- DNS Domains: resolution of app-specific domains (e.g., signal.org, telegram.org, whatsapp.net)
- ASN (Autonomous System Number): network infrastructure identification (e.g., AS32934 for Meta/ Facebook/WhatsApp)
- Traffic Patterns: detection of characteristic application patterns (e.g., STUN on ports 3478/19302 for WebRTC)
- Protocols: analysis of transport and application protocols (TCP/UDP, TLS, HTTP, XMPP, STUN)

Each attribution includes a confidence level (0-100%) based on the strength of evidence collected.

TLS Fingerprints Analysis (JA3/JA4)

Summary of TLS fingerprint analysis extracted from network traffic. JA3/JA4 fingerprints allow identification of TLS clients and servers regardless of IP or domain.

413	50	8	0
TLS Connections	Unique JA3	Unique JA4	IOC Matches

Metric	Value	Description
TLS Connections Analyzed	413	Total connections with extracted fingerprints
JA3 Fingerprints (Client)	67	Fingerprints identifying the TLS client
Unique JA3 Fingerprints	50	Different client profiles observed
JA4 Fingerprints	67	Next-gen fingerprints (more accurate)
Unique JA4 Fingerprints	8	Different JA4 profiles observed
JA4S Fingerprints (Server)	67	TLS server responses
Unique SNI Destinations	32	Distinct destination domains
Unique Destination IPs	45	Distinct server IPs contacted

No fingerprints match known malicious IOCs
All analyzed fingerprints appear legitimate according to the IOC database.

File Transfer Analysis

Files detected in network traffic and correlated with responsible applications.

Application	Risk	File	Size	Destination	Hash
Unknown	Moderate Score: 50	application/x-xz	4.4 MB	34.104.35.123Port 80	SHA1 13c9155b238f…
Unknown	Moderate Score: 40	application/x-xz	5.8 KB	34.104.35.123Port 80	SHA1 9ae4d226d3e3…
Unknown	Moderate Score: 40	application/chrome-ext	328.2 KB	34.104.35.123Port 80	SHA1 9baa8dbe7d69…
Unknown	Moderate Score: 40	application/x-xz	8.5 KB	34.104.35.123Port 80	SHA1 226425f83603…
Unknown	Moderate Score: 40	application/chrome-ext	5.3 KB	34.104.35.123Port 80	SHA1 4b5a01cfea4c…
Unknown	Moderate Score: 40	application/chrome-ext	5.8 KB	34.104.35.123Port 80	SHA1 bd4942b347b1…
Unknown	Moderate Score: 40	application/chrome-ext	65.1 KB	34.104.35.123Port 80	SHA1 b48d37db8116…
Unknown	Moderate Score: 40	text/json	94 B	45.207.207.168Port 80	SHA1 66afc3c43220…
Unknown	Moderate Score: 40	text/json	564 B	45.207.207.168Port 80	SHA1 cb06bd7395c6…
Unknown	Moderate Score: 40		2 B	45.207.207.168Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	1.3 KB	45.207.207.168Port 80	SHA1 51e2d79d5fdf…

Application	Risk	File	Size	Destination	Hash
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	56 B	45.207.200.251Port 80	SHA1 22caa57059df…
Unknown	Moderate Score: 40	text/json	94 B	45.207.200.251Port 80	SHA1 66afc3c43220…
Unknown	Moderate Score: 40	text/json	549 B	45.207.200.251Port 80	SHA1 9bebbe6b6d61…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	1.3 KB	45.207.200.251Port 80	SHA1 63383f0e0929…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	56 B	45.207.200.251Port 80	SHA1 121e58a01f89…
Unknown	Moderate Score: 40	text/json	94 B	45.207.200.251Port 80	SHA1 1bc33578f251…
Unknown	Moderate Score: 40	text/json	549 B	45.207.200.251Port 80	SHA1 be4a99173635…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	1.3 KB	45.207.200.251Port 80	SHA1 fb22efceef2f…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…

Application	Risk	File	Size	Destination	Hash
Unknown	Moderate Score: 40	text/json	1.3 KB	45.207.200.251Port 80	SHA1 ea5c6219ca51…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	1.3 KB	45.207.200.251Port 80	SHA1 43dd0f1eec2b…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	56 B	45.207.200.251Port 80	SHA1 03ee2694bb20…
Unknown	Moderate Score: 40	text/json	94 B	45.207.200.251Port 80	SHA1 1bc33578f251…
Unknown	Moderate Score: 40	text/json	549 B	45.207.200.251Port 80	SHA1 c1e4307a0a51…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	1.3 KB	45.207.200.251Port 80	SHA1 208560c2678d…
Unknown	Moderate Score: 40		2 B	45.207.200.251Port 80	SHA1 bf21a9e8fbc5…
Unknown	Moderate Score: 40	text/json	56 B	45.207.200.251Port 80	SHA1 5794e39964eb…
Unknown	Moderate Score: 40	application/x-xz	33.4 KB	34.104.35.123Port 80	SHA1 6c7b23fcbcda…
Unknown	Moderate Score: 40	application/x-xz	6.4 KB	34.104.35.123Port 80	SHA1 d7c6d6502505…

Application	Risk	File	Size	Destination	Hash
Unknown	Moderate Score: 40	application/chrome-ext	609.9 KB	34.104.35.123Port 80	SHA1 9fa16259f974...
Unknown	Moderate Score: 40	application/x-xz	246.7 KB	34.104.35.123Port 80	SHA1 db57b7e1d4ae...

TLS Certificate Characteristics

Analysis of TLS certificate characteristics observed in traffic. Technical observations are presented with their confidence level.

Evaluation	Server / Port	Certificate	TLS	Technical Observations
LOW Score: 15	nfc.nfu829.com 43.153.232.152:443	nfc.nfu829.comIssuer: TrustAsia DV TLS RSA CA 2025	TLS 1.2	• +5 Free certificate (CN=TrustAsia DV TLS RSA CA 2025,O=TrustAsia Technologies\\, Inc.,C=CN) • +10 Unknown application with certificate anomalies

Forensic Analysis - Alternative Hypotheses

Framework OIHL (Observation-Interpretation-Hypothesis-Likelihood)
Each indicator is analyzed according to forensic methodology that separates objective facts from interpretations and presents alternative hypotheses (legitimate and potentially malicious) with their respective probabilities. This approach ensures defensible conclusions based on evidence.

Overall Assessment

Risk Level: CRITICAL
Recommended Action: Immediate Isolation
Isolate device immediately and preserve evidence for forensic analysis.

Finding: 14 total
• High priority: 14

• Medium priority: 0
• Low priority: 0

Critical threat detected: 11 critical findings, active C2 communication suspected.

101.32.207.8:8080

CRITICAL (0% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑37.7 KB ↓16.7 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http,websocket. verso 101.32.207.8:8080. con 38571 bytes inviati e 17071 bytes ricevuti.

Alternative Hypotheses:

⚠	Esfiltrazione dati	56%
	Cloud backup (Google Drive, iCloud, OneDrive)	11%
	Videochiamata con camera attiva	11%
	Condivisione file (WhatsApp, Telegram)	11%
	Telemetria/Analytics legittima	11%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

101.32.207.8:8080

CRITICAL (0% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑37.7 KB ↓16.7 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso 101.32.207.8:8080. con 38571 bytes inviati e 17071 bytes ricevuti.

Alternative Hypotheses:

⚠	Esfiltrazione dati	56%
	Cloud backup (Google Drive, iCloud, OneDrive)	11%
	Videochiamata con camera attiva	11%
	Condivisione file (WhatsApp, Telegram)	11%
	Telemetria/Analytics legittima	11%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

154.90.54.222:8080

CRITICAL (0% conf)

Enrichment: Geo: Seychelles | ASN: AS138915 | Bytes: ↑3.6 KB ↓1.2 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso 154.90.54.222:8080. con 3672 bytes inviati e 1233 bytes ricevuti.

Alternative Hypotheses:

⚠	Esfiltrazione dati	56%
	Cloud backup (Google Drive, iCloud, OneDrive)	11%
	Videochiamata con camera attiva	11%
	Condivisione file (WhatsApp, Telegram)	11%
	Telemetria/Analytics legittima	11%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

43.157.1.82:8080 CRITICAL (0% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑3.6 KB ↓1.2 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso 43.157.1.82:8080. con 3672 bytes inviati e 1233 bytes ricevuti.

Alternative Hypotheses:

⚠ Esfiltrazione dati 56%

Cloud backup (Google Drive, iCloud, OneDrive) 11%

Videochiamata con camera attiva 11%

Condivisione file (WhatsApp, Telegram) 11%

Telemetria/Analytics legittima 11%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

43.157.184.190:8080 CRITICAL (0% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑4.2 KB ↓1.2 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso 43.157.184.190:8080. con 4312 bytes inviati e 1233 bytes ricevuti.

Alternative Hypotheses:

⚠ Esfiltrazione dati 56%

Cloud backup (Google Drive, iCloud, OneDrive) 11%

Videochiamata con camera attiva 11%

Condivisione file (WhatsApp, Telegram) 11%

Telemetria/Analytics legittima 11%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

43.159.143.39:8080 CRITICAL (0% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑14.4 KB ↓8.9 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso 43.159.143.39:8080. con 14780 bytes inviati e 9140 bytes ricevuti.

Alternative Hypotheses:

⚠ Spyware o malware 65%

App legittima non nel database 12%

SDK/libreria di terze parti 12%

Traffico di sistema Android/iOS 12%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

43.159.143.39:8080

CRITICAL (0% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑14.4 KB ↓8.9 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http,websocket. verso 43.159.143.39:8080. con 14780 bytes inviati e 9140 bytes ricevuti.

Alternative Hypotheses:

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

43.160.255.143:8080

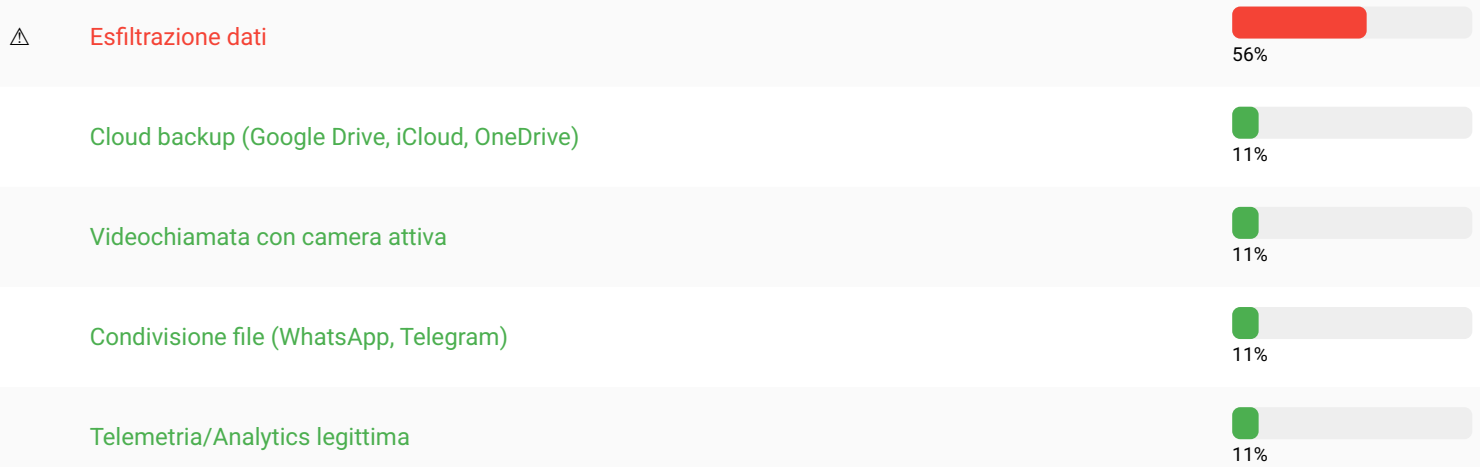
CRITICAL (0% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑4.0 KB ↓1.2 KB

App: Unknown (0% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso 43.160.255.143:8080. con 4120 bytes inviati e 1233 bytes ricevuti.

Alternative Hypotheses:



Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

app.nfuenglish2025.com (45.207.207.168:80) CRITICAL (33% conf)

Enrichment: Geo: MU | ASN: AS8796 | Bytes: ↑1.2 KB ↓1.9 KB

App: Unknown (33% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso app.nfuenglish2025.com (45.207.207.168:80). con 1224 bytes inviati e 1987 bytes ricevuti.

Alternative Hypotheses:

⚠ Spyware o malware 65%

App legittima non nel database 12%

SDK/libreria di terze parti 12%

Traffico di sistema Android/iOS 12%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

app.nfuenglish2025.com (45.207.207.168:80) CRITICAL (33% conf)

Enrichment: Geo: MU | ASN: AS8796 | Bytes: ↑1.2 KB ↓1.9 KB

App: Unknown (33% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso app.nfuenglish2025.com (45.207.207.168:80). con 1224 bytes inviati e 1987 bytes ricevuti.

Alternative Hypotheses:

⚠ Spyware o malware 65%

App legittima non nel database 12%

SDK/libreria di terze parti 12%

Traffico di sistema Android/iOS 12%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

app.nfuenglish2025.com (45.207.200.251:80) CRITICAL (33% conf)

Enrichment: Geo: MU | ASN: AS8796 | Bytes: ↑6.7 KB ↓10.1 KB

App: Unknown (33% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso app.nfuenglish2025.com (45.207.200.251:80). con 6886 bytes inviati e 10360 bytes ricevuti.

Alternative Hypotheses:

⚠ Spyware o malware 65%

App legittima non nel database 12%

SDK/libreria di terze parti 12%

Traffico di sistema Android/iOS 12%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

app.nfuenglish2025.com (45.207.200.251:80)

CRITICAL (33% conf)

Enrichment: Geo: MU | ASN: AS8796 | Bytes: ↑6.7 KB ↓10.1 KB

App: Unknown (33% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso app.nfuenglish2025.com (45.207.200.251:80). con 6886 bytes inviati e 10360 bytes ricevuti.

Alternative Hypotheses:

⚠	Spyware o malware	65%
	App legittima non nel database	12%
	SDK/libreria di terze parti	12%
	Traffico di sistema Android/iOS	12%

Conclusion: ⚠ Requires investigation: Threat level CRITICAL determined by Senior Forensic Engine (MITRE: T1041, T1071)

nfc.nfu829.com (43.153.232.152:443)

MEDIUM (33% conf)

Enrichment: Geo: Singapore | ASN: AS132203 | Bytes: ↑7.5 KB ↓9.7 MB

App: Unknown (33% attribution) | Proto: TCP

Observation: Connessione TCP/ssl. verso nfc.nfu829.com (43.153.232.152:443). con 7658 bytes inviati e 10180622 bytes ricevuti.

Alternative Hypotheses:

	App legittima non nel database	40%
	SDK/libreria di terze parti	30%
	Traffico di sistema Android/iOS	15%
⚠	Spyware o malware	15%

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

ws.rc8820.com (43.159.99.24:8080) HIGH (28% conf)

Enrichment: Geo: Singapore | ASN: AS139341 | Bytes: ↑2.4 KB ↓1.4 KB

App: Unknown (28% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso ws.rc8820.com (43.159.99.24:8080). con 2440 bytes inviati e 1472 bytes ricevuti.

Alternative Hypotheses:

⚠	Spyware o malware	65%
	App legittima non nel database	12%
	SDK/libreria di terze parti	12%

Traffico di sistema Android/iOS

12%

Conclusion: ⚠ Requires investigation: Threat level HIGH determined by Senior Forensic Engine (MITRE: T1041, T1071)

ws.rc8820.com (43.159.98.31:8080)

MEDIUM (28% conf)

Enrichment: Geo: Singapore | ASN: AS139341 | Bytes: ↑180 B ↓92 B

App: Unknown (28% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso ws.rc8820.com (43.159.98.31:8080). con 180 bytes inviati e 92 bytes ricevuti.

Alternative Hypotheses:

App legittima non nel database

40%

SDK/libreria di terze parti

30%

Traffico di sistema Android/iOS

15%

⚠ Spyware o malware

15%

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

edgedl.me.gvt1.com (34.104.35.123:80)

MEDIUM (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑3.7 KB ↓5.7 MB

App: Unknown (50% attribution) | Proto: TCP

Observation: Connessione TCP/http. verso edgedl.me.gvt1.com (34.104.35.123:80). con 3825 bytes inviati e 6004064 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

	App legittima non nel database	40%
	SDK/libreria di terze parti	30%
	Traffico di sistema Android/iOS	15%
⚠	Spyware o malware	15%

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

events.swishapps.ai (34.150.232.69:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑6.3 KB ↓5.8 KB

App: Unknown (50% attribution) | Proto: TCP

Observation: Connessione TCP/ssl. verso events.swishapps.ai (34.150.232.69:443). con 6442 bytes inviati e 5890 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

App legittima non nel database 40%

SDK/libreria di terze parti 30%

Traffico di sistema Android/iOS 15%

⚠ Spyware o malware 15%

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

lh3.googleusercontent.com (142.250.114.132:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑12.7 KB ↓159.6 KB

App: Twitter (33% attribution) | Proto: UDP

Observation: Connessione UDP/quic,ssl. verso lh3.googleusercontent.com (142.250.114.132:443). con 12999 bytes inviati e 163387 bytes ricevuti.

Alternative Hypotheses:

App legittima non nel database 40%

SDK/libreria di terze parti 30%

Traffico di sistema Android/iOS 15%

⚠ Spyware o malware 15%

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

Uncategorized Communications

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
UDP	dns	--	10.10.2.1	53	↑2.5KB ↓7.4KB	--
TCP	tcp	--	10.10.2.101	37304	↑827B ↓66B	--
TCP	ssl	--	142.251.186.94	443	↑1.6KB ↓7.0KB	--
TCP	tls	--	173.194.208.94	443	↑152B ↓184B	--
UDP	quic,ssl	accounts.google.com	142.251.186.84	443	↑5.9KB ↓10.4KB	--
TCP	ssl	android-safebrowsing.google.com	142.251.116.91	443	↑9.8KB ↓16.6KB	--
UDP	quic,ssl	android-safebrowsing.google.com	142.251.116.91	443	↑9.8KB ↓16.6KB	--
UDP	quic,ssl	clients4.google.com	142.251.186.102	443	↑14.7KB ↓20.0KB	--
TCP	ssl	clients4.google.com	142.251.186.102	443	↑14.7KB ↓20.0KB	--
TCP	ssl	de0mpg.cdn-settings.appsflyersdk.com	143.204.130.117	443	↑921B ↓5.4KB	--
UDP	quic,ssl	digitalassetlinks.googleapis.com	192.178.220.95	443	↑9.2KB ↓16.7KB	--
TCP	ssl	digitalassetlinks.googleapis.com	192.178.220.95	443	↑9.2KB ↓16.7KB	--
TCP	ssl	events.swishapps.ai	34.150.232.69	443	↑6.3KB ↓5.8KB	--
TCP	tls	firebase-settings.crashlytics.com	142.250.113.94	443	↑24.9KB ↓28.5KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	firebase-settings.crashlytics.com	142.250.113.94	443	↑24.9KB ↓28.5KB	--
UDP	quic,ssl	firebase-settings.crashlytics.com	142.250.113.94	443	↑24.9KB ↓28.5KB	--
TCP	ssl	inbox.google.com	142.250.113.17	443	↑2.93MB ↓119.2KB	--
TCP	ssl	infinitedata-pa.googleapis.com	142.250.113.95	443	↑8.2KB ↓21.9KB	--
TCP	ssl	infinitedata-pa.googleapis.com	142.250.115.95	443	↑12.2KB ↓20.3KB	--
TCP	tls	infinitedata-pa.googleapis.com	142.250.138.95	443	↑63B ↓73B	--
TCP	tls	infinitedata-pa.googleapis.com	142.251.116.95	443	↑42.6KB ↓224.8KB	--
TCP	ssl	infinitedata-pa.googleapis.com	142.250.114.95	443	↑7.6KB ↓12.1KB	--
TCP	ssl	infinitedata-pa.googleapis.com	142.251.116.95	443	↑42.6KB ↓224.8KB	--
UDP	quic,ssl	infinitedata-pa.googleapis.com	142.250.115.95	443	↑12.2KB ↓20.3KB	--
UDP	quic,ssl	infinitedata-pa.googleapis.com	142.251.116.95	443	↑42.6KB ↓224.8KB	--
UDP	quic,ssl	infinitedata-pa.googleapis.com	173.194.208.95	443	↑54.0KB ↓53.0KB	--
UDP	quic,ssl	lh3.googleusercontent.com	142.250.114.132	443	↑12.7KB ↓159.6KB	--
TCP	ssl	mail.google.com	142.251.186.83	443	↑6.6KB ↓13.6KB	--
TCP	ssl	mail.google.com	142.251.186.17	443	↑3.1KB ↓12.5KB	--
TCP	ssl	play-fe.googleapis.com	142.250.113.139	443	↑11.0KB ↓8.0KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	play.google.com	142.250.138.139	443	↑862B ↓11.1KB	--
UDP	quic,ssl	play.google.com	142.250.138.102	443	↑12.8KB ↓15.6KB	--
TCP	ssl	play.googleapis.com	216.239.32.223	443	↑95.6KB ↓38.4KB	--
UDP	quic,ssl	play.googleapis.com	216.239.32.223	443	↑95.6KB ↓38.4KB	--
TCP	ssl	pro-client-config.swishapps.ai	34.8.241.29	443	↑908B ↓5.2KB	--
TCP	ssl	sdk-01.moengage.com	13.32.104.125	443	↑2.9KB ↓5.6KB	--
TCP	ssl	update.googleapis.com	142.250.114.94	443	↑19.4KB ↓21.8KB	--
UDP	quic,ssl	update.googleapis.com	142.250.114.94	443	↑19.4KB ↓21.8KB	--
TCP	ssl	vzwappprofile.vzw.com	23.206.56.116	443	↑1.2KB ↓5.5KB	--
UDP	ipsec	wo.vzwwo.com	141.207.227.233	500	↑1.7KB ↓1.7KB	--
UDP	ipsec	wo.vzwwo.com	141.207.227.233	4500	↑13.8KB ↓9.3KB	--
TCP	tls	www.facebook.com	157.240.24.35	443	↑1.1KB ↓5.5KB	--
TCP	ssl	www.facebook.com	157.240.24.35	443	↑1.1KB ↓5.5KB	--
UDP	quic,ssl	www.google.com	142.251.116.99	443	↑5.1KB ↓5.2KB	--
TCP	ssl	www.google.com	142.250.114.105	443	↑7.1KB ↓13.8KB	--
UDP	quic,ssl	www.google.com	142.250.114.105	443	↑7.1KB ↓13.8KB	--

Whitelisted communications

Protocol	Domain	Dst IP address	Dst port number
UDP	--	10.10.2.1	53
TCP	--	10.10.2.101	37304
TCP	--	142.251.186.94	443
TCP	--	173.194.208.94	443
UDP	accounts.google.com	142.251.186.84	443
TCP	android-safebrowsing.google.com	142.251.116.91	443
UDP	android-safebrowsing.google.com	142.251.116.91	443
UDP	clients4.google.com	142.251.186.102	443
TCP	clients4.google.com	142.251.186.102	443
TCP	de0mpg.cdn-settings.appsflyersdk.com	143.204.130.117	443
UDP	digitalassetlinks.googleapis.com	192.178.220.95	443
TCP	digitalassetlinks.googleapis.com	192.178.220.95	443
TCP	edgedl.me.gvt1.com	34.104.35.123	80
TCP	edgedl.me.gvt1.com	34.104.35.123	443
TCP	events.swishapps.ai	34.150.232.69	443
TCP	firebase-settings.crashlytics.com	142.250.113.94	443

Protocol	Domain	Dst IP address	Dst port number
TCP	firebase-settings.crashlytics.com	142.250.113.94	443
UDP	firebase-settings.crashlytics.com	142.250.113.94	443
TCP	inbox.google.com	142.250.113.17	443
TCP	infinitedata-pa.googleapis.com	142.250.113.95	443
TCP	infinitedata-pa.googleapis.com	142.250.115.95	443
TCP	infinitedata-pa.googleapis.com	142.250.138.95	443
TCP	infinitedata-pa.googleapis.com	142.251.116.95	443
TCP	infinitedata-pa.googleapis.com	142.250.114.95	443
TCP	infinitedata-pa.googleapis.com	142.251.116.95	443
UDP	infinitedata-pa.googleapis.com	142.250.115.95	443
UDP	infinitedata-pa.googleapis.com	142.251.116.95	443
UDP	infinitedata-pa.googleapis.com	173.194.208.95	443
UDP	lh3.googleusercontent.com	142.250.114.132	443
TCP	mail.google.com	142.251.186.83	443
TCP	mail.google.com	142.251.186.17	443
TCP	play-fe.googleapis.com	142.250.113.139	443
TCP	play.google.com	142.250.138.139	443
UDP	play.google.com	142.250.138.102	443

Protocol	Domain	Dst IP address	Dst port number
TCP	play.googleapis.com	216.239.32.223	443
UDP	play.googleapis.com	216.239.32.223	443
TCP	pro-client-config.swishapps.ai	34.8.241.29	443
TCP	sdk-01.moengage.com	13.32.104.125	443
TCP	update.googleapis.com	142.250.114.94	443
UDP	update.googleapis.com	142.250.114.94	443
TCP	vzwappprofile.vzw.com	23.206.56.116	443
UDP	wo.vzwwo.com	141.207.227.233	500
UDP	wo.vzwwo.com	141.207.227.233	4500
TCP	www.facebook.com	157.240.24.35	443
TCP	www.facebook.com	157.240.24.35	443
UDP	www.google.com	142.251.116.99	443
TCP	www.google.com	142.250.114.105	443
UDP	www.google.com	142.250.114.105	443