INDEX

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: Markus
Device description: Work Device
Report generated on 16/01/2026 - 19:26:10
Capture duration: 609.752266 seconds
Number of packets: 35433
Capture SHA1: 580df5a4878ecec545e24ddd5070b039d7afdbeb

Analysis Result

Detected one high-priority indicator requiring in-depth analysis.

Conclusions

Quantitative Summary

Analysis identified: 1 high-priority indicator, 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: 1 critical finding, 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	`client.mobilefonex.com`	client.mobilefonex.com	T1417.001 Keylogging	60%

MITRE ATT&CK Analysis

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

Critical Findings with ATT&CK Mapping

client.mobilefonex.com CRITICAL

Confidence: 60.0% (95% CI: 45.0% - 75.0%) | Kill Chain: Command & Control

Techniques: T1417.001

⚡ Recommended Action: Investigate Keylogging - Detected 12 small POST requests (avg 16 bytes, interval 44.9s) to client.mobilefonex.com

STIX 2.1 Export Available

Threat intelligence bundle generated for sharing:

- 1 Indicators (IOC)
- 1 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

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

T1417.001	Keylogging	1	Indirect

Evidence Details (IP/Domain)

Technique	Target IP	Target Domain	Confidence	Evidence
T1417.001 Keylogging	client.mobilefonex.com	client.mobilefonex.com	60%	Detected 12 small POST requests (avg 16 bytes, interval 44.9s) to client.mobilef

PCAP Observability Classification

Indirect

1

Inferable from network patterns

T1417.001

Mobile Tactics Observed

Mobile tactics identified via network traffic analysis:

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	33%	MODERATE	c.bing.com 204.79.197.200:443	TCP ssl	↑ 1.2 KB ↓ 8.3 KB	No TLS SNI, DNS, or temporal correlation evidence for 204.79.197.200:443 DNS: c.bing.com, PORT: 443

MODERATE 2x Alerts: CERT-02, FILE-06

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
⚠ Vulnerability/Threat: Risk score: 50/100. Factors: SNI 'c.bing.com' != CN 'www.bing.com' (domain fronting indicator); Validation error: unable to get local issuer certificate; Unknown application with certificate anomalies | SNI: c.bing.com						
Unknown	33%	MODERATE	hbopenbid.pubmatic.com 103.231.98.193:443	TCP ssl	↑ 12.8 KB ↓ 14.1 KB	No TLS SNI, DNS, or temporal correlation evidence for 103.231.98.193:443 DNS: hbopenbid.pubmatic.com, PORT: 443
MODERATE CERT-01 ⚠ Vulnerability/Threat: Risk score: 50/100. Factors: Self-signed certificate detected; Unknown application with certificate anomalies | SNI: hbopenbid.pubmatic.com						
Unknown	33%	MODERATE	image4.pubmatic.com 103.231.98.195:443	TCP ssl	↑ 2.6 KB ↓ 10.6 KB	No TLS SNI, DNS, or temporal correlation evidence for 103.231.98.195:443 DNS: image4.pubmatic.com, PORT: 443
MODERATE CERT-01 ⚠ Vulnerability/Threat: Risk score: 50/100. Factors: Self-signed certificate detected; Unknown application with certificate anomalies | SNI: image4.pubmatic.com						
Unknown	33%	MODERATE	image6.pubmatic.com 103.231.98.196:443	TCP ssl	↑ 1.6 KB ↓ 11.4 KB	No TLS SNI, DNS, or temporal correlation evidence for 103.231.98.196:443 DNS: image6.pubmatic.com, PORT: 443
MODERATE CERT-01 ⚠ Vulnerability/Threat: Risk score: 50/100. Factors: Self-signed certificate detected; Unknown application with certificate anomalies | SNI: image6.pubmatic.com						

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
Unknown	50%	MODERATE	match.prod.bidr.io 54.236.195.76:443	TCP ssl	↑ 5.4 KB ↓ 19.3 KB	No TLS/DNS evidence for 54.236.195.76:443 on Infrastructure ASN: Amazon (AS14618) DNS: match.prod.bidr.io, ASN: Infrastructure ASN: Amazon (AS14618), PORT: 443

MODERATE CERT-02

⚠ Vulnerability/Threat: Risk score: 55/100. Factors: SNI 'match.prod.bidr.io' != CN '*.match.prod.bidr.io' (domain fronting indicator); Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US; Unknown application with certificate anomalies | SNI: match.prod.bidr.io

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
Unknown	50%	MODERATE	rtb.adentifi.com 54.174.34.153:443	TCP ssl	↑ 2.0 KB ↓ 11.7 KB	No TLS/DNS evidence for 54.174.34.153:443 on Infrastructure ASN: Amazon (AS14618) DNS: rtb.adentifi.com, ASN: Infrastructure ASN: Amazon (AS14618), PORT: 443

MODERATE CERT-02

⚠ Vulnerability/Threat: Risk score: 55/100. Factors: SNI 'rtb.adentifi.com' != CN 'adentifi.com' (domain fronting indicator); Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US; Unknown application with certificate anomalies | SNI: rtb.adentifi.com

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
Unknown	33%	MODERATE	simage2.pubmatic.com 103.231.98.194:443	TCP ssl	↑ 10.9 KB ↓ 31.9 KB	No TLS SNI, DNS, or temporal correlation evidence for 103.231.98.194:443 DNS: image2.pubmatic.com, PORT: 443

MODERATE CERT-01

⚠ Vulnerability/Threat: Risk score: 50/100. Factors: Self-signed certificate detected; Unknown application with certificate anomalies | SNI: simage2.pubmatic.com

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
Unknown	33%	MODERATE	simage2.pubmatic.com 103.231.98.194:443	TCP tls	↑ 10.9 KB ↓ 31.9 KB	No TLS SNI, DNS, or temporal correlation evidence for 103.231.98.194:443 DNS: image2.pubmatic.com, PORT: 443
MODERATE	CERT-01	⚠ Vulnerability/Threat: Risk score: 50/100. Factors: Self-signed certificate detected; Unknown application with certificate anomalies | SNI: simage2.pubmatic.com				
Unknown	33%	MODERATE	simage4.pubmatic.com 67.199.150.85:443	TCP ssl	↑ 3.1 KB ↓ 9.3 KB	No TLS SNI, DNS, or temporal correlation evidence for 67.199.150.85:443 DNS: simage4.pubmatic.com, PORT: 443
MODERATE	CERT-01	⚠ Vulnerability/Threat: Risk score: 50/100. Factors: Self-signed certificate detected; Unknown application with certificate anomalies | SNI: simage4.pubmatic.com				
Unknown	33%	LOW	62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com 199.127.194.97:443	TCP ssl	↑ 6.8 KB ↓ 11.8 KB	No TLS SNI, DNS, or temporal correlation evidence for 199.127.194.97:443 DNS: 62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com, PORT: 443
LOW	CERT-02	⚠ Vulnerability/Threat: Risk score: 45/100. Factors: SNI '62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com' != CN 'cws.conviva.com' (domain fronting indicator); Free certificate (CN=Sectigo RSA Organization Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB); Unknown application with certificate anomalies | SNI: 62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com				
Unknown	33%	LOW	62ea30a39dede4f6d44ac289591051076c	TCP ssl	↑ 4.0 KB ↓ 21.2 KB	No TLS SNI, DNS, or temporal correlation evidence for 199.127.193.108:443

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
			294526.cws.conviva.com 199.127.193.108:443			DNS: 62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com, PORT: 443

LOW CERT-02

⚠ Vulnerability/Threat: Risk score: 45/100. Factors: SNI '62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com' != CN 'cws.conviva.com' (domain fronting indicator); Free certificate (CN=Sectigo RSA Organization Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB); Unknown application with certificate anomalies | SNI: 62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com

Unknown	50%	LOW	aax-eu.amazon-adsystem.com 54.239.38.253:443	TCP ssl	↑ 9.4 KB ↓ 16.0 KB	No TLS/DNS evidence for 54.239.38.253:443 on Infrastructure ASN: Amazon (AS16509) DNS: aax-eu.amazon-adsystem.com, ASN: Infrastructure ASN: Amazon (AS16509), PORT: 443

LOW FILE-06

⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 54.239.38.253 via Unknown

Unknown	33%	LOW	acdn.adnxs.com 151.101.141.108:443	TCP ssl	↑ 1.2 KB ↓ 22.8 KB	No TLS SNI, DNS, or temporal correlation evidence for 151.101.141.108:443 DNS: acdn.adnxs.com, PORT: 443

LOW 2x Alerts: CERT-02, FILE-06

⚠ Vulnerability/Threat: File '' (1.4KB) uploaded to 151.101.141.108 via Unknown

Unknown	33%	LOW	ads.pubmatic.com 104.122.80.250:443	TCP ssl	↑ 3.0 KB ↓ 30.3 KB	No TLS SNI, DNS, or temporal correlation evidence for 104.122.80.250:443 DNS: ads.pubmatic.com, PORT: 443

LOW FILE-06

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 104.122.80.250 via Unknown						
Unknown	33%	LOW	ae.linkedin.com 144.2.15.5:443	TCP ssl	↑ 1.7 KB ↓ 14.1 KB	No TLS SNI, DNS, or temporal correlation evidence for 144.2.15.5:443 DNS: ae.linkedin.com, PORT: 443
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 40/100. Factors: SNI 'ae.linkedin.com' != CN 'us.linkedin.com' (domain fronting indicator); Unknown application with certificate anomalies | SNI: ae.linkedin.com						
Unknown	33%	LOW	bttrack.com 192.132.33.46:443	TCP ssl	↑ 2.3 KB ↓ 9.9 KB	No TLS SNI, DNS, or temporal correlation evidence for 192.132.33.46:443 DNS: bttrack.com, PORT: 443
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 45/100. Factors: SNI 'bttrack.com' != CN '*.bttrack.com' (domain fronting indicator); Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB); Unknown application with certificate anomalies | SNI: bttrack.com						
Unknown	33%	LOW	c1.adform.net 185.84.60.20:443	TCP tls	↑ 6.2 KB ↓ 21.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 185.84.60.20:443 DNS: c1.adform.net, PORT: 443
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 40/100. Factors: SNI 'c1.adform.net' != CN 'track.adform.net' (domain fronting indicator); Unknown application with certificate anomalies | SNI: c1.adform.net						
Unknown	33%	LOW	c1.adform.net 185.84.60.20:443	TCP ssl	↑ 6.2 KB ↓ 21.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 185.84.60.20:443 DNS: c1.adform.net, PORT: 443

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 40/100. Factors: SNI 'c1.adform.net' != CN 'track.adform.net' (domain fronting indicator); Unknown application with certificate anomalies | SNI: c1.adform.net						
Unknown	50%	LOW	cdn.ampproject.org `142.250.200.193:443`	TCP ssl	↑ 11.3 KB ↓ 1.2 MB	No TLS/DNS evidence for 142.250.200.193:443 on Infrastructure ASN: Google (AS15169) DNS: cdn.ampproject.org, ASN: Infrastructure ASN: Google (AS15169), PORT: 443
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 45/100. Factors: SNI 'cdn.ampproject.org' != CN 'misc-sni.google.com' (domain fronting indicator); Free certificate (CN=GTS CA 1C3,O=Google Trust Services LLC,C=US); Unknown application with certificate anomalies | SNI: cdn.ampproject.org						
Unknown	33%	LOW	client.mobilefonex.com `159.138.146.100:80`	TCP http	↑ 7.9 KB ↓ 3.6 KB	No TLS SNI, DNS, or temporal correlation evidence for 159.138.146.100:80 DNS: client.mobilefonex.com, PORT: 80
LOW 36x FILE-06 ⚠ Vulnerability/Threat: File '' (0.0KB) uploaded to 159.138.146.100 via Unknown						
Unknown	33%	LOW	cm.adgrx.com `63.251.232.170:443`	TCP ssl	↑ 1.9 KB ↓ 13.4 KB	No TLS SNI, DNS, or temporal correlation evidence for 63.251.232.170:443 DNS: cm.adgrx.com, PORT: 443
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 45/100. Factors: SNI 'cm.adgrx.com' != CN 'public1.adgear.com' (domain fronting indicator); Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB); Unknown application with certificate anomalies | SNI: cm.adgrx.com						

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
Unknown	33%	LOW	edge.api.brightcove.com 151.101.142.27:443	TCP ssl	↑ 1.9 KB ↓ 13.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 151.101.142.27:443 DNS: edge.api.brightcove.com, PORT: 443
LOW	3x	Alerts: CERT-02, FILE-06				
⚠ Vulnerability/Threat: File '' (1.4KB) uploaded to 151.101.142.27 via Unknown						
Unknown	33%	LOW	htlb.casalemedia.com 2.21.111.28:443	TCP ssl	↑ 6.0 KB ↓ 15.3 KB	No TLS SNI, DNS, or temporal correlation evidence for 2.21.111.28:443 DNS: htlb.casalemedia.com, PORT: 443
LOW	4x	Alerts: CERT-02, FILE-06				
⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 2.21.111.28 via Unknown						
Unknown	33%	LOW	htlb.casalemedia.com 2.21.111.28:443	TCP tls	↑ 6.0 KB ↓ 15.3 KB	No TLS SNI, DNS, or temporal correlation evidence for 2.21.111.28:443 DNS: htlb.casalemedia.com, PORT: 443
LOW	4x	Alerts: CERT-02, FILE-06				
⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 2.21.111.28 via Unknown						
Unknown	33%	LOW	ib.adnxs.com 185.33.220.216:443	TCP ssl	↑ 13.7 KB ↓ 18.5 KB	No TLS SNI, DNS, or temporal correlation evidence for 185.33.220.216:443 DNS: secure.adnxs.com, PORT: 443
LOW	3x	FILE-06				
⚠ Vulnerability/Threat: File '' (0.3KB) uploaded to 185.33.220.216 via Unknown						
Unknown	33%	LOW	ib.adnxs.com 185.33.221.53:443		↑ 2.3 KB ↓ 5.0 KB	No TLS SNI, DNS, or temporal correlation evidence for 185.33.221.53:443

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
				TCP ssl		DNS: secure.adnxs.com, PORT: 443
LOW FILE-06 ⚠ Vulnerability/Threat: File '' (0.3KB) uploaded to 185.33.221.53 via Unknown						
Unknown	33%	LOW	id5-sync.com `51.89.21.5:443`	TCP ssl	↑ 3.3 KB ↓ 8.5 KB	No TLS SNI, DNS, or temporal correlation evidence for 51.89.21.5:443 DNS: id5-sync.com, PORT: 443
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 45/100. Factors: SNI 'id5-sync.com' != CN '*.id5-sync.com' (domain fronting indicator); Free certificate (CN=R3,O=Let's Encrypt,C=US); Unknown application with certificate anomalies | SNI: id5-sync.com						
Google	50%	LOW	inbox.google.com `172.217.171.197:443`	TCP ssl	↑ 6.9 KB ↓ 25.0 KB	TLS SNI direct match: inbox.google.com SNI: inbox.google.com, PORT: 443
LOW CERT-02 ⚠ Vulnerability/Threat: Risk score: 35/100. Factors: SNI 'inbox.google.com' != CN 'mail.google.com' (domain fronting indicator); Free certificate (CN=GTS CA 1C3,O=Google Trust Services LLC,C=US) | SNI: inbox.google.com | App: Google						
Unknown	33%	LOW	js-sec.indexww.com `104.122.81.53:443`	TCP ssl	↑ 34.9 KB ↓ 67.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 104.122.81.53:443 DNS: ssum.casalemedia.com, PORT: 443
LOW 7x Alerts: CERT-02, FILE-06 ⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 104.122.81.53 via Unknown						

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
Unknown	50%	LOW	s.amazon-adsystem.com 209.54.180.3:443	TCP ssl	↑ 4.9 KB ↓ 17.1 KB	No TLS/DNS evidence for 209.54.180.3:443 on Infrastructure ASN: Amazon (AS16509) DNS: s.amazon-adsystem.com, ASN: Infrastructure ASN: Amazon (AS16509), PORT: 443
LOW	2x	FILE-06	⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 209.54.180.3 via Unknown			
Unknown	33%	LOW	sync-tm.everesttech.net 199.232.82.49:443	TCP ssl	↑ 2.2 KB ↓ 10.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 199.232.82.49:443 DNS: sync-tm.everesttech.net, PORT: 443
LOW	2x	FILE-06	⚠ Vulnerability/Threat: File '' (1.4KB) uploaded to 199.232.82.49 via Unknown			
Unknown	33%	LOW	sync.inmobi.com 20.72.149.136:443	TCP ssl	↑ 1.9 KB ↓ 15.1 KB	No TLS SNI, DNS, or temporal correlation evidence for 20.72.149.136:443 DNS: sync.inmobi.com, PORT: 443
LOW	2x	FILE-06	⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 20.72.149.136 via Unknown			
Unknown	33%	LOW	sync.technoratimedia.com 193.122.130.38:443	TCP ssl	↑ 1.9 KB ↓ 7.0 KB	No TLS SNI, DNS, or temporal correlation evidence for 193.122.130.38:443 DNS: sync.technoratimedia.com, PORT: 443
LOW	2x	FILE-06	⚠ Vulnerability/Threat: File '' (0.3KB) uploaded to 193.122.130.38 via Unknown			

App	Score	Alert	DESTINATION	PROTOCOL	Bytes (↑up ↓down)	REASON
Unknown	33%	LOW	um.simpli.fi 169.50.137.184:443	TCP ssl	↑ 2.9 KB ↓ 13.7 KB	No TLS SNI, DNS, or temporal correlation evidence for 169.50.137.184:443 DNS: um.simpli.fi, PORT: 443
LOW	3x	FILE-06	⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 169.50.137.184 via Unknown			
Unknown	33%	LOW	vjs.zencdn.net 151.101.142.217:443	TCP ssl	↑ 1.6 KB ↓ 17.3 KB	No TLS SNI, DNS, or temporal correlation evidence for 151.101.142.217:443 DNS: vjs.zencdn.net, PORT: 443
LOW	2x	FILE-06	⚠ Vulnerability/Threat: File '' (1.4KB) uploaded to 151.101.142.217 via Unknown			
Unknown	33%	LOW	www.linkedin.com 13.107.42.14:443	TCP ssl	↑ 25.7 KB ↓ 40.1 KB	No TLS SNI, DNS, or temporal correlation evidence for 13.107.42.14:443 DNS: px.ads.linkedin.com, PORT: 443
LOW	3x	FILE-06	⚠ Vulnerability/Threat: File '' (0.5KB) uploaded to 13.107.42.14 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 (2 flows)

Total flows: 158 | Average confidence: 33%

Protocols	Domains	ASN	IP Addresses
tcp	62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com a.pub.network a.tribalfusion.com aax-eu.amazon-adsystem.com acdn.adnxs.com ad-delivery.net ad.doubleclick.net ad.turn.com ads.creative-serving.com ads.playground.xyz	--	10.215.173.2 103.231.98.193 103.231.98.194 103.231.98.195 103.231.98.196 104.122.80.180 104.122.80.250 104.122.80.29 104.122.81.100 104.122.81.53

Detailed Flows (Forensic View) - Grouped by Domain

⚠ djp.bz (1 flows)

Status	Proto	Destination	Bytes	Evidence
⚠	tcp:443	djp.bz	↑1.1KB ↓274B	No TLS SNI, DNS, or temporal correlation...

⚠ mpnijffhvaxs (1 flows)

Status	Proto	Destination	Bytes	Evidence
⚠	tcp:80	mpnijffhvaxs	↑660B ↓160B	No TLS SNI, DNS, or temporal correlation...

✓ sharethrough.com (9 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	btlr.sharethrough.com	↑5.0KB ↓28.8KB	No TLS/DNS evidence for 54.255.100.22:44...
✓	tcp:443	btlr.sharethrough.com	↑5.0KB ↓28.8KB	No TLS/DNS evidence for 54.255.100.22:44...
✓	tcp:443	btlr.sharethrough.com	↑4.2KB ↓17.7KB	No TLS/DNS evidence for 54.251.155.125:4...
✓	tcp:443	btlr.sharethrough.com	↑4.2KB ↓17.7KB	No TLS/DNS evidence for 54.251.155.125:4...
✓	tcp:443	btlr.sharethrough.com	↑1.6KB ↓10.5KB	No TLS/DNS evidence for 52.220.250.98:44...
✓	tcp:443	btlr.sharethrough.com	↑1.6KB ↓10.5KB	No TLS/DNS evidence for 52.220.250.98:44...
✓	tcp:443	match.sharethrough.com	↑3.0KB ↓14.1KB	No TLS/DNS evidence for 52.77.1.3:443 on...
✓	tcp:443	match.sharethrough.com	↑3.3KB ↓5.9KB	No TLS/DNS evidence for 35.156.177.8:443...
✓	tcp:443	match.sharethrough.com	↑3.3KB ↓5.9KB	No TLS/DNS evidence for 35.156.177.8:443...

✓ doubleclick.net (8 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ad.doubleclick.net	↑1.7KB ↓10.8KB	No TLS/DNS evidence for 142.251.37.198:4...
✓	tcp:443	googleads.g.doubleclick.net	↑18.8KB ↓77.2KB	No TLS/DNS evidence for 172.217.18.34:44...
✓	tcp:443	googleads.g.doubleclick.net	↑18.8KB ↓77.2KB	No TLS/DNS evidence for 172.217.18.34:44...
✓	tcp:443	googleads.g.doubleclick.net	↑6.5KB ↓29.3KB	No TLS/DNS evidence for 142.250.201.34:4...
✓	tcp:443	googleads.g.doubleclick.net	↑3.4KB ↓14.7KB	No TLS/DNS evidence for 142.251.37.162:4...
✓	tcp:443	securepubads.g.doubleclick.net	↑31.0KB ↓240.4KB	No TLS/DNS evidence for 172.217.171.226:...

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	securepubads.g.doubleclick.net	↑31.0KB ↓240.4KB	No TLS/DNS evidence for 172.217.171.226:...
✓	tcp:443	stats.g.doubleclick.net	↑3.2KB ↓7.8KB	No TLS/DNS evidence for 108.177.15.157:4...

✓ pubmatic.com (7 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ads.pubmatic.com	↑3.0KB ↓30.3KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	hbopenbid.pubmatic.com	↑12.8KB ↓14.1KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	image4.pubmatic.com	↑2.6KB ↓10.6KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	image6.pubmatic.com	↑1.6KB ↓11.4KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	simage2.pubmatic.com	↑10.9KB ↓31.9KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	simage2.pubmatic.com	↑10.9KB ↓31.9KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	simage4.pubmatic.com	↑3.1KB ↓9.3KB	No TLS SNI, DNS, or temporal correlation...

✓ googlesyndication.com (6 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pagead2.googlesyndication.com	↑7.5KB ↓9.0KB	No TLS/DNS evidence for 142.251.37.194:4...
✓	tcp:443	pagead2.googlesyndication.com	↑7.6KB ↓78.4KB	No TLS/DNS evidence for 142.250.203.226:...
✓	tcp:443	pagead2.googlesyndication.com	↑10.7KB ↓25.3KB	No TLS/DNS evidence for 172.217.21.2:443...
✓	tcp:443	pagead2.googlesyndication.com	↑10.7KB ↓25.3KB	No TLS/DNS evidence for 172.217.21.2:443...

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	tpc.googlesyndication.com	↑5.1KB ↓85.1KB	No TLS/DNS evidence for 216.58.212.97:44...
✓	tcp:443	tpc.googlesyndication.com	↑1.4KB ↓24.2KB	No TLS/DNS evidence for 142.250.185.97:4...

✓ IP/ASN (5 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:53	10.215.173.2	↑10.3KB ↓26.3KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	142.250.200.226	↑2.3KB ↓1.4KB	No TLS/DNS evidence for 142.250.200.226:...
✓	tcp:443	62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com	↑6.8KB ↓11.8KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com	↑4.0KB ↓21.2KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:53	8.8.8.8	↑717B ↓848B	No TLS/DNS evidence for 8.8.8.8:53 on In...

✓ amazon-adsystem.com (4 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	aax-eu.amazon-adsystem.com	↑9.4KB ↓16.0KB	No TLS/DNS evidence for 54.239.38.253:44...
✓	tcp:443	c.amazon-adsystem.com	↑7.0KB ↓71.9KB	No TLS/DNS evidence for 52.222.142.111:4...
✓	tcp:443	c.amazon-adsystem.com	↑3.9KB ↓7.9KB	No TLS SNI, DNS, or temporal correlation...

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	s.amazon-adsystem.com	↑4.9KB ↓17.1KB	No TLS/DNS evidence for 209.54.180.3:443...

✓ xiaomi.net (4 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:5222	app.chat.global.xiaomi.net	↑1.1KB ↓171B	No TLS SNI, DNS, or temporal correlation...
✓	tcp:5222	app.chat.global.xiaomi.net	↑1.1KB ↓171B	No TLS SNI, DNS, or temporal correlation...
✓	tcp:5222	app.chat.global.xiaomi.net	↑1.1KB ↓183B	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	resolver.msg.global.xiaomi.net	↑1.1KB ↓3.9KB	No TLS SNI, DNS, or temporal correlation...

✓ criteo.com (4 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	bidder.criteo.com	↑11.4KB ↓23.7KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	bidder.criteo.com	↑11.4KB ↓23.7KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	dis.criteo.com	↑1.8KB ↓7.3KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	gum.criteo.com	↑4.3KB ↓17.5KB	No TLS SNI, DNS, or temporal correlation...

✓ adnxs.com (3 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	acdn.adnxs.com	↑1.2KB ↓22.8KB	No TLS SNI, DNS, or temporal correlation...

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ib.adnxs.com	↑13.7KB ↓18.5KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	ib.adnxs.com	↑2.3KB ↓5.0KB	No TLS SNI, DNS, or temporal correlation...

✓ brightcove.com (3 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	edge.api.brightcove.com	↑1.9KB ↓13.7KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	metrics.brightcove.com	↑23.1KB ↓21.4KB	No TLS/DNS evidence for 35.244.232.184:4...
✓	tcp:443	metrics.brightcove.com	↑23.1KB ↓21.4KB	No TLS/DNS evidence for 35.244.232.184:4...

✓ yahoo.com (3 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pr-bh.ybp.yahoo.com	↑2.2KB ↓12.4KB	No TLS/DNS evidence for 54.75.169.44:443...
✓	tcp:443	pr-bh.ybp.yahoo.com	↑2.2KB ↓12.4KB	No TLS/DNS evidence for 54.75.169.44:443...
✓	tcp:443	ups.analytics.yahoo.com	↑2.9KB ↓14.7KB	No TLS/DNS evidence for 18.156.0.31:443 ...

✓ quantserve.com (3 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	secure.quantserve.com	↑2.7KB ↓18.2KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	secure.quantserve.com	↑2.0KB ↓6.0KB	No TLS SNI, DNS, or temporal correlation...

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	secure.quantserve.com	↑2.0KB ↓6.0KB	No TLS SNI, DNS, or temporal correlation...

✓ bidswitch.net (3 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	x.bidswitch.net	↑12.2KB ↓14.5KB	No TLS/DNS evidence for 3.121.19.101:443...
✓	tcp:443	x.bidswitch.net	↑2.4KB ↓10.6KB	No TLS/DNS evidence for 18.185.222.19:44...
✓	tcp:443	x.bidswitch.net	↑2.4KB ↓10.6KB	No TLS/DNS evidence for 18.185.222.19:44...

✓ pub.network (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	a.pub.network	↑1.3KB ↓353.1KB	No TLS/DNS evidence for 104.26.0.139:443...
✓	tcp:443	d.pub.network	↑39.0KB ↓47.3KB	No TLS/DNS evidence for 35.201.71.192:44...

✓ tribalfusion.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	a.tribalfusion.com	↑4.4KB ↓8.6KB	No TLS/DNS evidence for 104.18.13.5:443 ...
✓	tcp:443	a.tribalfusion.com	↑4.4KB ↓8.6KB	No TLS/DNS evidence for 104.18.13.5:443 ...

✓ yieldmo.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ads.yieldmo.com	↑6.5KB ↓17.4KB	No TLS/DNS evidence for 54.254.235.164:4...
✓	tcp:443	ads.yieldmo.com	↑3.0KB ↓11.4KB	No TLS/DNS evidence for 3.1.139.153:443 ...

✓ linkedin.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ae.linkedin.com	↑1.7KB ↓14.1KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	www.linkedin.com	↑25.7KB ↓40.1KB	No TLS SNI, DNS, or temporal correlation...

✓ btloader.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	api.btloader.com	↑1.1KB ↓5.3KB	No TLS/DNS evidence for 130.211.23.194:4...
✓	tcp:443	btloader.com	↑990B ↓33.4KB	No TLS/DNS evidence for 172.67.70.134:44...

✓ rlcdn.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	api.rlcdn.com	↑1.0KB ↓6.9KB	No TLS/DNS evidence for 34.120.155.137:4...
✓	tcp:443	id.rlcdn.com	↑3.0KB ↓21.2KB	No TLS/DNS evidence for 35.190.60.146:44...

✓ deployads.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	c.deployads.com	↑10.4KB ↓30.8KB	No TLS/DNS evidence for 52.205.117.34:44...
✓	tcp:443	c.deployads.com	↑6.1KB ↓18.0KB	No TLS/DNS evidence for 54.220.62.216:44...

✓ adform.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	c1.adform.net	↑6.2KB ↓21.7KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	c1.adform.net	↑6.2KB ↓21.7KB	No TLS SNI, DNS, or temporal correlation...

✓ dotomi.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	casale-match.dotomi.com	↑3.0KB ↓12.0KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	casale-match.dotomi.com	↑3.0KB ↓12.0KB	No TLS SNI, DNS, or temporal correlation...

✓ cookielaw.org (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	cdn.cookielaw.org	↑3.7KB ↓164.2KB	No TLS/DNS evidence for 104.16.148.64:44...
✓	tcp:443	cdn.cookielaw.org	↑3.7KB ↓164.2KB	No TLS/DNS evidence for 104.16.148.64:44...

✓ id5-sync.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	cdn.id5-sync.com	↑1.6KB ↓20.1KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	id5-sync.com	↑3.3KB ↓8.5KB	No TLS SNI, DNS, or temporal correlation...

✓ mobilefonex.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:80	client.mobilefonex.com	↑7.9KB ↓3.6KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	push.mobilefonex.com	↑6.3KB ↓32.9KB	No TLS SNI, DNS, or temporal correlation...

✓ media.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	cs.media.net	↑2.2KB ↓10.0KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	cs.media.net	↑2.2KB ↓10.0KB	No TLS SNI, DNS, or temporal correlation...

✓ aljazeera.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	dsportal.aljazeera.net	↑8.4KB ↓6.8KB	No TLS/DNS evidence for 104.18.26.213:44...
✓	tcp:443	www.aljazeera.net	↑30.3KB ↓1.36MB	No TLS SNI, DNS, or temporal correlation...

✓ openx.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	freestar-d.openx.net	↑7.5KB ↓22.7KB	No TLS/DNS evidence for 35.244.159.8:443...
✓	tcp:443	rtb.openx.net	↑1.9KB ↓8.3KB	No TLS/DNS evidence for 35.227.252.103:4...

✓ casalemedia.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	htlb.casalemedia.com	↑6.0KB ↓15.3KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	htlb.casalemedia.com	↑6.0KB ↓15.3KB	No TLS SNI, DNS, or temporal correlation...

✓ crwdcntrl.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	id.crwdcntrl.net	↑1.1KB ↓6.7KB	No TLS/DNS evidence for 18.139.37.129:44...
✓	tcp:443	sync.crwdcntrl.net	↑1.9KB ↓11.9KB	No TLS/DNS evidence for 52.76.4.134:443 ...

✓ getaj.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	live-hls-web-aja.getaj.net	↑19.5KB ↓9.25MB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	live-hls-web-aja.getaj.net	↑19.5KB ↓9.25MB	No TLS SNI, DNS, or temporal correlation...

✓ chartbeat.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ping.chartbeat.net	↑4.6KB ↓8.4KB	No TLS/DNS evidence for 23.20.220.210:44...
✓	tcp:443	ping.chartbeat.net	↑2.3KB ↓7.4KB	No TLS/DNS evidence for 3.211.176.233:44...

✓ licdn.com (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	static-exp1.licdn.com	↑1.8KB ↓38.7KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	static-exp1.licdn.com	↑14.3KB ↓420.0KB	No TLS SNI, DNS, or temporal correlation...

✓ criteo.net (2 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	static.criteo.net	↑5.2KB ↓44.3KB	No TLS SNI, DNS, or temporal correlation...
✓	tcp:443	static.criteo.net	↑5.2KB ↓44.3KB	No TLS SNI, DNS, or temporal correlation...

✓ ad-delivery.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ad-delivery.net	↑1.6KB ↓6.1KB	No TLS/DNS evidence for 104.26.2.70:443 ...

✓ turn.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ad.turn.com	↑2.4KB ↓15.2KB	No TLS SNI, DNS, or temporal correlation...

✓ creative-serving.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ads.creative-serving.com	↑4.3KB ↓20.5KB	No TLS/DNS evidence for 3.120.18.167:443...

✓ playground.xyz (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	ads.playground.xyz	↑1.7KB ↓11.1KB	No TLS/DNS evidence for 34.102.253.54:44...

✓ xiaomi.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	api.ad.intl.xiaomi.com	↑990B ↓3.6KB	No TLS SNI, DNS, or temporal correlation...

✓ zemanta.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	b1sync.zemanta.com	↑3.6KB ↓10.6KB	No TLS SNI, DNS, or temporal correlation...

✓ nr-data.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	bam.nr-data.net	↑33.0KB ↓11.1KB	No TLS SNI, DNS, or temporal correlation...

✓ bttrack.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	bttrack.com	↑2.3KB ↓9.9KB	No TLS SNI, DNS, or temporal correlation...

✓ bing.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	c.bing.com	↑1.2KB ↓8.3KB	No TLS SNI, DNS, or temporal correlation...

✓ ampproject.org (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	cdn.ampproject.org	↑11.3KB ↓1.23MB	No TLS/DNS evidence for 142.250.200.193:...

✓ adgrx.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	cm.adgrx.com	↑1.9KB ↓13.4KB	No TLS SNI, DNS, or temporal correlation...

✓ iprom.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	core.iprom.net	↑1.9KB ↓9.6KB	No TLS SNI, DNS, or temporal correlation...

✓ loopme.me (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	csync.loopme.me	↑1.8KB ↓9.5KB	No TLS SNI, DNS, or temporal correlation...

✓ adsrvr.org (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	data.adsrvr.org	↑4.4KB ↓20.6KB	No TLS/DNS evidence for 15.197.193.217:4...

✓ brand-display.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	dmp.brand-display.com	↑1.1KB ↓4.4KB	No TLS/DNS evidence for 34.111.151.213:4...

✓ cinarra.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	dps.jp.cinarra.com	↑1.9KB ↓12.3KB	No TLS/DNS evidence for 18.179.236.28:44...

✓ videoplayerhub.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	freestar-io.videoplayerhub.com	↑1.6KB ↓5.7KB	No TLS/DNS evidence for 172.67.74.207:44...

✓ appier.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	gocm.c.appier.net	↑1.6KB ↓10.6KB	No TLS SNI, DNS, or temporal correlation...

✓ dyntrk.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	gu.dyntrk.com	↑2.1KB ↓11.4KB	No TLS SNI, DNS, or temporal correlation...

✓ sharedid.org (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	id.sharedid.org	↑1.7KB ↓11.6KB	No TLS/DNS evidence for 52.10.19.115:443...

✓ newrelic.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	js-agent.newrelic.com	↑989B ↓19.3KB	No TLS SNI, DNS, or temporal correlation...

✓ indexww.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	js-sec.indexww.com	↑34.9KB ↓67.7KB	No TLS SNI, DNS, or temporal correlation...

✓ exelator.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	loadm.exelator.com	↑2.0KB ↓7.5KB	No TLS/DNS evidence for 52.26.6.186:443 ...

✓ bidr.io (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	match.prod.bidr.io	↑5.4KB ↓19.3KB	No TLS/DNS evidence for 54.236.195.76:44...

✓ ensighten.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	nexus.ensighten.com	↑2.2KB ↓32.1KB	No TLS/DNS evidence for 52.209.177.22:44...

✓ adsymptotic.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	p.adsymptotic.com	↑2.8KB ↓7.6KB	No TLS/DNS evidence for 104.18.98.194:44...

✓ rfihub.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	p.rfihub.com	↑2.1KB ↓7.3KB	No TLS SNI, DNS, or temporal correlation...

✓ googleadservices.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pagead2.googleadservices.com	↑9.1KB ↓5.0KB	No TLS/DNS evidence for 142.250.200.194:...

✓ pghub.io (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pghub.io	↑1.6KB ↓12.1KB	No TLS/DNS evidence for 35.241.45.217:44...

✓ pippio.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pippio.com	↑2.0KB ↓11.2KB	No TLS/DNS evidence for 107.178.254.65:4...

✓ tapad.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pixel.tapad.com	↑1.6KB ↓5.0KB	No TLS/DNS evidence for 35.227.248.159:4...

✓ brightcove.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	players.brightcove.net	↑1.0KB ↓243.6KB	No TLS SNI, DNS, or temporal correlation...

✓ w55c.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pm.w55c.net	↑4.6KB ↓18.8KB	No TLS/DNS evidence for 13.228.74.15:443...

✓ admedo.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pool.admedo.com	↑2.7KB ↓13.5KB	No TLS/DNS evidence for 35.210.53.219:44...

✓ ip-api.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	pro.ip-api.com	↑2.4KB ↓6.0KB	No TLS SNI, DNS, or temporal correlation...

✓ adentifi.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	rtb.adentifi.com	↑2.0KB ↓11.7KB	No TLS/DNS evidence for 54.174.34.153:44...

✓ gumgum.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	rtb.gumgum.com	↑1.8KB ↓11.4KB	No TLS/DNS evidence for 54.178.144.187:4...

✓ scorecardresearch.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sb.scorecardresearch.com	↑2.5KB ↓9.2KB	No TLS/DNS evidence for 52.222.137.28:44...

✓ fastclick.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	secure.cdn.fastclick.net	↑1.6KB ↓25.3KB	No TLS SNI, DNS, or temporal correlation...

✓ bluekai.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	stags.bluekai.com	↑2.6KB ↓11.1KB	No TLS SNI, DNS, or temporal correlation...

✓ ad-m.asia (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sync-dsp.ad-m.asia	↑2.0KB ↓7.1KB	No TLS SNI, DNS, or temporal correlation...

✓ everesttech.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sync-tm.everesttech.net	↑2.2KB ↓10.7KB	No TLS SNI, DNS, or temporal correlation...

✓ 1rx.io (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sync.1rx.io	↑7.5KB ↓22.2KB	No TLS SNI, DNS, or temporal correlation...

✓ inmobi.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sync.inmobi.com	↑1.9KB ↓15.1KB	No TLS SNI, DNS, or temporal correlation...

✓ mathtag.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sync.mathtag.com	↑7.1KB ↓14.0KB	No TLS SNI, DNS, or temporal correlation...

✓ technoratimedia.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	sync.technoratimedia.com	↑1.9KB ↓7.0KB	No TLS SNI, DNS, or temporal correlation...

✓ linksynergy.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	tags.rd.linksynergy.com	↑1.6KB ↓9.4KB	No TLS/DNS evidence for 34.98.67.3:443 o...

✓ taboola.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	trc.taboola.com	↑2.1KB ↓9.1KB	No TLS SNI, DNS, or temporal correlation...

✓ semasio.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	uipglob.semasio.net	↑2.3KB ↓7.5KB	No TLS SNI, DNS, or temporal correlation...

✓ simpli.fi (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	um.simpli.fi	↑2.9KB ↓13.7KB	No TLS SNI, DNS, or temporal correlation...

✓ zencdn.net (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	vjs.zencdn.net	↑1.6KB ↓17.3KB	No TLS SNI, DNS, or temporal correlation...

✓ googletagmanager.com (1 flows)

Status	Proto	Destination	Bytes	Evidence
✓	tcp:443	www.googletagmanager.com	↑1.7KB ↓81.0KB	No TLS/DNS evidence for 142.251.37.40:44...

Google ✓ - Legitimate

Total flows: 43 | Average confidence: 97%

Protocols	Domains	ASN	IP Addresses
tcp, udp	accounts.google.com adservice.google.com adservice.google.jo android.googleapis.com connectivitycheck.gstatic.com dialercallinfolookup-pa.googleapis.com encrypted-tbn0.gstatic.com fonts.gstatic.com google.com id.google.com	--	108.177.15.188 142.250.181.226 142.250.186.132 142.250.200.195 142.250.200.202 142.250.200.234 142.250.201.14 142.250.201.3 142.251.117.94 142.251.37.163

Detailed Flows (Forensic View)

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	accounts.google.com (172.217.19.141)	↑2.0KB ↓3.5KB	TLS SNI direct match: accounts.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	adservice.google.com (172.217.18.226)	↑3.3KB ↓10.8KB	TLS SNI direct match: adservice.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	adservice.google.com (142.250.181.226)	↑1.6KB ↓3.1KB	TLS SNI direct match: adservice.google.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	adservice.google.jo (172.217.171.194)	↑4.4KB ↓15.3KB	TLS SNI direct match: adservice.google.jo
2022-03-1309:38:41	✓ Legitimate	tcp/tls:443	adservice.google.jo (172.217.171.194)	↑4.4KB ↓15.3KB	TLS SNI direct match: adservice.google.jo
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	android.googleapis.com (172.217.171.202)	↑1.8KB ↓2.0KB	TLS SNI direct match: android.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	connectivitycheck.gstatic.com (142.251.37.163)	↑1.1KB ↓1.3KB	TLS SNI direct match: connectivitycheck.gstatic.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	connectivitycheck.gstatic.com (142.250.201.3)	↑1.9KB ↓2.1KB	TLS SNI direct match: connectivitycheck.gstatic.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	dialercallinfolookup-pa.googleapis.com (172.217.18.234)	↑25.6KB ↓135.9KB	TLS SNI direct match: dialercallinfolookup-pa.googleapis.com
2022-03-1309:38:41	✓ Legitimate	udp/tls: 443	dialercallinfolookup-pa.googleapis.com (172.217.18.234)	↑25.6KB ↓135.9KB	TLS SNI direct match: dialercallinfolookup-pa.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/tls:443	encrypted-tbn0.gstatic.com (216.58.198.78)	↑4.6KB ↓70.8KB	TLS SNI direct match: encrypted-tbn0.gstatic.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	encrypted-tbn0.gstatic.com (216.58.198.78)	↑4.6KB ↓70.8KB	TLS SNI direct match: encrypted-tbn0.gstatic.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	fonts.gstatic.com (142.250.200.195)	↑1.8KB ↓33.6KB	TLS SNI direct match: fonts.gstatic.com
2022-03-1309:38:41	✓ Legitimate	tcp/http:80	google.com (172.217.171.238)	↑533B ↓616B	DNS correlation: google.com → 172.217.171.238
2022-03-1309:38:41	✓ Legitimate	tcp/http:80	google.com (172.217.171.238)	↑533B ↓616B	DNS correlation: google.com → 172.217.171.238
2022-03-1309:38:41		tcp/ssl:443			TLS SNI direct match: id.google.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
	✓ Legitimate		id.google.com (142.251.117.94)	↑2.2KB ↓15.3KB	
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	inbox.google.com (172.217.171.197)	↑6.9KB ↓25.0KB	TLS SNI direct match: inbox.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 5228	mtalk.google.com (173.194.76.188)	↑959B ↓850B	TLS SNI direct match: mtalk.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 5228	mtalk.google.com (108.177.15.188)	↑988B ↓876B	TLS SNI direct match: mtalk.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 5228	mtalk.google.com (74.125.206.188)	↑4.7KB ↓4.1KB	TLS SNI direct match: mtalk.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 5228	mtalk.google.com (64.233.184.188)	↑3.0KB ↓2.6KB	TLS SNI direct match: mtalk.google.com
2022-03-1309:38:41	✓ Legitimate	tcp:5228	mtalk.google.com (64.233.184.188)	↑3.0KB ↓2.6KB	TLS SNI direct match: mtalk.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	ssl.gstatic.com (142.251.37.227)	↑584B ↓5.7KB	TLS SNI direct match: ssl.gstatic.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	ssl.gstatic.com (172.217.171.227)	↑8.5KB ↓77.5KB	TLS SNI direct match: www.google.jo
2022-03-1309:38:41	✓ Legitimate	udp/tls: 443	www.google.com (142.251.37.36)	↑23.2KB ↓9.5KB	TLS SNI direct match: www.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.google.com (142.251.37.36)	↑23.2KB ↓9.5KB	TLS SNI direct match: www.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.google.com (172.217.21.4)	↑34.6KB ↓1.32MB	TLS SNI direct match: www.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.google.com (142.250.186.132)	↑2.5KB ↓2.0KB	TLS SNI direct match: www.google.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	udp/ quic,ssl: 443	www.googleapis.com (142.250.200.202)	↑20.0KB ↓10.8KB	TLS SNI direct match: content-autofill.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.googleapis.com (142.251.37.202)	↑10.8KB ↓3.6KB	TLS SNI direct match: play.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.googleapis.com (172.217.171.234)	↑3.9KB ↓13.3KB	TLS SNI direct match: android.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.googleapis.com (142.251.37.42)	↑8.4KB ↓20.3KB	TLS SNI direct match: safebrowsing.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.googleapis.com (142.250.200.234)	↑656B ↓820B	TLS SNI direct match: fonts.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.googleapis.com (142.250.200.202)	↑20.0KB ↓10.8KB	TLS SNI direct match: content-autofill.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.googleapis.com (216.58.198.74)	↑1.8KB ↓3.7KB	TLS SNI direct match: fonts.googleapis.com
2022-03-1309:38:41	✓ Legitimate	udp/ quic,ssl: 443	www.googleapis.com (142.251.37.42)	↑8.4KB ↓20.3KB	TLS SNI direct match: safebrowsing.googleapis.com
2022-03-1309:38:41	✓ Legitimate	tcp/tls:443	www.gstatic.com (216.58.198.67)	↑4.8KB ↓90.2KB	TLS SNI direct match: www.gstatic.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.gstatic.com (216.58.198.67)	↑4.8KB ↓90.2KB	TLS SNI direct match: www.gstatic.com
2022-03-1309:38:41	✓ Legitimate	udp/tls: 443	www.youtube.com (216.58.211.206)	↑7.7KB ↓36.0KB	DNS correlation: play-fe.googleapis.com → 216.58.211.206
2022-03-1309:38:41	✓ Legitimate	udp/tls: 443	www.youtube.com (172.217.18.46)	↑3.9KB ↓6.8KB	DNS correlation: android.clients.google.com → 172.217.18.46

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.youtube.com (142.250.201.14)	↑1.9KB ↓47.1KB	TLS SNI direct match: apis.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.youtube.com (142.251.37.206)	↑3.5KB ↓16.6KB	TLS SNI direct match: play.google.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.youtube.com (172.217.21.14)	↑1.6KB ↓8.2KB	TLS SNI direct match: encrypted-tbn0.gstatic.com

Twitter ✓ - Legitimate

Total flows: 29 | Average confidence: 99%

Protocols	Domains	ASN	IP Addresses
tcp, udp	ap.lijit.com app-measurement.com beacons.gcp.gvt2.com eb2.3lift.com eus.rubiconproject.com fastlane.rubiconproject.com geolocation.onetrust.com ipac.ctnsnet.com lh5.googleusercontent.com mab.chartbeat.com	--	10.215.173.2 104.117.200.100 104.20.184.68 13.227.217.7 13.248.245.213 142.250.185.110 142.250.203.246 142.251.37.194 151.101.2.202 169.197.150.8

Detailed Flows (Forensic View)

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	udp/ dns:53	10.215.173.2	↑10.3KB ↓26.3KB	UDP flow inherited context from TLS SNI: lh5.googleuserco...
2022-03-1309:38:41			8.8.8.8		

Timestamp	Status	Proto	Destination	Bytes	Evidence
	✓ Legitimate	udp/ dns:53		↑717B ↓848B	UDP flow inherited context from TLS SNI: lh5.googleuserco...
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	ap.lijit.com (72.251.249.14)	↑10.7KB ↓21.5KB	TLS SNI direct match: ap.lijit.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	ap.lijit.com (72.251.249.13)	↑4.8KB ↓18.3KB	TLS SNI direct match: ce.lijit.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	ap.lijit.com (209.191.163.210)	↑5.6KB ↓14.0KB	TLS SNI direct match: ap.lijit.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	app-measurement.com (142.250.185.110)	↑2.2KB ↓1.1KB	TLS SNI direct match: app-measurement.com
2022-03-1309:38:41	✓ Legitimate	udp/tls: 443	beacons.gcp.gvt2.com (172.217.18.227)	↑8.1KB ↓3.4KB	UDP flow inherited context from TLS SNI: lh5.googleuserco...
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	eb2.3lift.com (13.248.245.213)	↑4.2KB ↓20.1KB	TLS SNI direct match: eb2.3lift.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	eus.rubiconproject.com (104.117.200.100)	↑2.4KB ↓15.3KB	TLS SNI direct match: eus.rubiconproject.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	fastlane.rubiconproject.com (213.19.162.31)	↑8.9KB ↓21.6KB	TLS SNI direct match: fastlane.rubiconproject.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	geolocation.onetrust.com (104.20.184.68)	↑1.6KB ↓5.7KB	TLS SNI direct match: geolocation.onetrust.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	ipac.ctnsnet.com (35.186.193.173)	↑1.8KB ↓8.2KB	TLS SNI direct match: ipac.ctnsnet.com
2022-03-1309:38:41	✓ Legitimate	tcp/tls: 443	lh5.googleusercontent.com (172.217.18.225)	↑2.6KB ↓52.7KB	TLS SNI direct match: lh5.googleusercontent.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	lh5.googleusercontent.com (172.217.18.225)	↑2.6KB ↓52.7KB	TLS SNI direct match: lh5.googleusercontent.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	mab.chartbeat.com (151.101.2.202)	↑1.1KB ↓5.5KB	TLS SNI direct match: mab.chartbeat.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	match.deepintent.com (169.197.150.8)	↑1.7KB ↓7.3KB	TLS SNI direct match: match.deepintent.com
2022-03-1309:38:41	✓ Legitimate	udp/tls: 443	pagead2.googlesyndication.com (142.251.37.194)	↑7.5KB ↓9.0KB	UDP flow inherited context from TLS SNI: lh5.googleuserco...
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	pixel-eu.rubiconproject.com (69.173.144.138)	↑2.1KB ↓6.7KB	TLS SNI direct match: pixel-eu.rubiconproject.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	pixel-eu.rubiconproject.com (69.173.144.165)	↑4.6KB ↓10.9KB	TLS SNI direct match: token.rubiconproject.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	pixel-eu.rubiconproject.com (69.173.144.139)	↑6.4KB ↓14.7KB	TLS SNI direct match: pixel.rubiconproject.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	pixel-sync.sitescout.com (66.155.71.150)	↑2.0KB ↓9.0KB	TLS SNI direct match: pixel-sync.sitescout.com
2022-03-1309:38:41	✓ Legitimate	tcp/tls: 443	pixel-sync.sitescout.com (66.155.71.25)	↑2.7KB ↓7.2KB	TLS SNI direct match: pixel-sync.sitescout.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	pixel-sync.sitescout.com (66.155.71.25)	↑2.7KB ↓7.2KB	TLS SNI direct match: pixel-sync.sitescout.com
2022-03-1309:38:41	✓ Legitimate	udp/tls: 443	play-lh.googleusercontent.com (142.250.203.246)	↑4.6KB ↓12.1KB	DNS correlation: play-lh.googleusercontent.com → 142.250....
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	rules.quantcount.com (52.222.137.87)	↑2.1KB ↓16.7KB	TLS SNI direct match: rules.quantcount.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	static.chartbeat.com (13.227.217.7)	↑2.1KB ↓34.1KB	TLS SNI direct match: static.chartbeat.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	tlx.3lift.com (54.93.106.38)	↑4.6KB ↓17.1KB	TLS SNI direct match: tlx.3lift.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	tlx.3lift.com (3.124.152.204)	↑2.8KB ↓11.9KB	TLS SNI direct match: tlx.3lift.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl: 443	www.youtube.com (172.217.19.46)	↑11.8KB ↓44.0KB	TLS SNI direct match: app-measurement.com

YouTube ✓ - Legitimate

Total flows: 5 | Average confidence: 100%

Protocols	Domains	ASN	IP Addresses
tcp, udp	i.ytimg.com www.youtube.com	--	142.250.201.46 142.251.37.214 216.58.205.214

Detailed Flows (Forensic View)

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	i.ytimg.com (142.251.37.214)	↑4.6KB ↓12.0KB	TLS SNI direct match: i.ytimg.com
2022-03-1309:38:41	✓ Legitimate	udp/tls:443	i.ytimg.com (142.251.37.214)	↑4.6KB ↓12.0KB	TLS SNI direct match: i.ytimg.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	i.ytimg.com (216.58.205.214)	↑2.4KB ↓22.1KB	TLS SNI direct match: i.ytimg.com
2022-03-1309:38:41	✓ Legitimate	tcp/ssl:443	www.youtube.com (142.250.201.46)	↑6.3KB ↓18.0KB	TLS SNI direct match: www.youtube.com
2022-03-1309:38:41	✓ Legitimate	udp/tls:443		↑6.3KB ↓18.0KB	TLS SNI direct match: www.youtube.com

Timestamp	Status	Proto	Destination	Bytes	Evidence
			www.youtube.com (142.250.201.46)		

WhatsApp ✓ - Legitimate

Total flows: 2 | Average confidence: 66%

Protocols	Domains	ASN	IP Addresses
tcp	g.whatsapp.net	–	157.240.195.54

Detailed Flows (Forensic View)

Timestamp	Status	Proto	Destination	Bytes	Evidence
2022-03-1309:38:41	✓ Legitimate	tcp/tls:443	g.whatsapp.net (157.240.195.54)	↑2.7KB ↓2.8KB	DNS correlation: g.whatsapp.net → 157.240.195.54
2022-03-1309:38:41	✓ Legitimate	tcp/xmpp:5222	g.whatsapp.net (157.240.195.54)	↑2.0KB ↓1.7KB	DNS correlation: g.whatsapp.net → 157.240.195.54

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.

959	17	17	0
TLS Connections	Unique JA3	Unique JA4	IOC Matches

Metric	Value	Description
TLS Connections Analyzed	959	Total connections with extracted fingerprints
JA3 Fingerprints (Client)	570	Fingerprints identifying the TLS client
Unique JA3 Fingerprints	17	Different client profiles observed
JA4 Fingerprints	570	Next-gen fingerprints (more accurate)
Unique JA4 Fingerprints	17	Different JA4 profiles observed
JA4S Fingerprints (Server)	570	TLS server responses
Unique SNI Destinations	177	Distinct destination domains
Unique Destination IPs	199	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: 40		23 B	159.138.146.100Port 80	SHA1 8ea5f869eeb9…
Unknown	Moderate Score: 40		120 B	159.138.146.100Port 80	SHA1 456b9a766776…
Unknown	Moderate Score: 40		253 B	159.138.146.100Port 80	SHA1 491b4e157305…
Unknown	Moderate Score: 40		33 B	159.138.146.100Port 80	SHA1 30f9599e1006…
Unknown	Moderate Score: 40		8 B	159.138.146.100Port 80	SHA1 461eebf88019…
Unknown	Moderate Score: 40		4 B	159.138.146.100Port 80	SHA1 f32cc36a3474…
Unknown	Moderate Score: 40		23 B	159.138.146.100Port 80	SHA1 301192d0c772…
Unknown	Moderate Score: 40		120 B	159.138.146.100Port 80	SHA1 c4dd158db249…
Unknown	Moderate Score: 40		301 B	159.138.146.100Port 80	SHA1 14b1c298372a…
Unknown	Moderate Score: 40		33 B	159.138.146.100Port 80	SHA1 ff2948716d94…
Unknown	Moderate Score: 40		8 B	159.138.146.100Port 80	SHA1 104f94e19f1b…

Application	Risk	File	Size	Destination	Hash
Unknown	Moderate Score: 40		4 B	159.138.146.100Port 80	SHA1 f32cc36a3474…
Unknown	Moderate Score: 40		23 B	159.138.146.100Port 80	SHA1 fca95b55dbf7…
Unknown	Moderate Score: 40		120 B	159.138.146.100Port 80	SHA1 1107fcd5ab30…
Unknown	Moderate Score: 40		269 B	159.138.146.100Port 80	SHA1 4180a0a0a8d2…
Unknown	Moderate Score: 40		33 B	159.138.146.100Port 80	SHA1 e647f8bdf601…
Unknown	Moderate Score: 40		8 B	159.138.146.100Port 80	SHA1 73267f784131…
Unknown	Moderate Score: 40		4 B	159.138.146.100Port 80	SHA1 f32cc36a3474…
Unknown	Moderate Score: 40		23 B	159.138.146.100Port 80	SHA1 cc050e55ba22…
Unknown	Moderate Score: 40		120 B	159.138.146.100Port 80	SHA1 19c754784990…
Unknown	Moderate Score: 40		285 B	159.138.146.100Port 80	SHA1 bea42597887f…
Unknown	Moderate Score: 40		33 B	159.138.146.100Port 80	SHA1 18b704c23a1e…
Unknown	Moderate Score: 40		8 B	159.138.146.100Port 80	SHA1 4d5d62e3d5df…
Unknown	Moderate Score: 40		4 B	159.138.146.100Port 80	SHA1 f32cc36a3474…

Application	Risk	File	Size	Destination	Hash
Google	LOW Score: 20	text/html	219 B	172.217.171.238Port 80	SHA1 c79f5572f672...
Unknown	LOW Score: 40	application/ocsp-response	471 B	www.linkedin.com13.107.42.14Port 443	SHA1 aee8808f374d...
Unknown	LOW Score: 40	application/ocsp-response	471 B	www.linkedin.com13.107.42.14Port 443	SHA1 aee8808f374d...
Twitter	LOW Score: 20	application/ocsp-response	1.4 KB	151.101.2.202Port 443	SHA1 8b8137f6e296...
Unknown	LOW Score: 40	application/ocsp-response	471 B	js-sec.indexww.com104.122.81.53Port 443	SHA1 b65d948a3029...
Unknown	LOW Score: 40	application/ocsp-response	471 B	js-sec.indexww.com104.122.81.53Port 443	SHA1 b65d948a3029...
Unknown	LOW Score: 40	application/ocsp-response	1.4 KB	vjs.zencdn.net151.101.142.217Port 443	SHA1 651a8058b8b7...
Unknown	LOW Score: 40	application/ocsp-response	1.4 KB	vjs.zencdn.net151.101.142.217Port 443	SHA1 651a8058b8b7...
Unknown	LOW Score: 40	application/ocsp-response	1.4 KB	edge.api.brightcove.com151.101.142.27Port 443	SHA1 bb6cba65f471...
Unknown	LOW Score: 40	application/ocsp-response	1.4 KB	edge.api.brightcove.com151.101.142.27Port 443	SHA1 bb6cba65f471...
Unknown	LOW Score: 40	application/ocsp-response	471 B	htlb.casalemedia.com2.21.111.28Port 443	SHA1 b65d948a3029...
Unknown	LOW Score: 40	application/ocsp-response	471 B	htlb.casalemedia.com2.21.111.28Port 443	SHA1 b65d948a3029...
Unknown	LOW Score: 40	application/ocsp-response	471 B	htlb.casalemedia.com2.21.111.28Port 443	SHA1 b65d948a3029...

Application	Risk	File	Size	Destination	Hash
Unknown	LOW Score: 40	application/ocsp-response	280 B	ib.adnxs.com185.33.220.216Port 443	SHA1 b5ec2e44ca75…
Unknown	LOW Score: 40	application/ocsp-response	280 B	ib.adnxs.com185.33.220.216Port 443	SHA1 b5ec2e44ca75…
Unknown	LOW Score: 40	application/ocsp-response	280 B	ib.adnxs.com185.33.220.216Port 443	SHA1 b5ec2e44ca75…
Unknown	LOW Score: 40	application/ocsp-response	471 B	aax-eu.amazon-adsystem.com54.239.38.253Port 443	SHA1 7b137ad4caac…
Unknown	LOW Score: 40	application/ocsp-response	471 B	ssum-sec.casalemedia.com104.122.81.53Port 443	SHA1 b65d948a3029…
Unknown	LOW Score: 40	application/ocsp-response	471 B	ads.pubmatic.com104.122.80.250Port 443	SHA1 2524f9fac537…
Unknown	LOW Score: 40	application/ocsp-response	472 B	sync.inmobi.com20.72.149.136Port 443	SHA1 6c81900881df…
Unknown	LOW Score: 40	application/ocsp-response	472 B	sync.inmobi.com20.72.149.136Port 443	SHA1 6c81900881df…
Unknown	LOW Score: 40	application/ocsp-response	471 B	ssum.casalemedia.com104.122.81.53Port 443	SHA1 b65d948a3029…
Unknown	LOW Score: 40	application/ocsp-response	471 B	dsum-sec.casalemedia.com104.122.81.53Port 443	SHA1 b65d948a3029…
Unknown	LOW Score: 40	application/ocsp-response	280 B	secure.adnxs.com185.33.221.53Port 443	SHA1 b5ec2e44ca75…
Unknown	LOW Score: 40	application/ocsp-response	471 B	s.amazon-adsystem.com209.54.180.3Port 443	SHA1 322928465d67…
Unknown	LOW Score: 40	application/ocsp-response	471 B	s.amazon-adsystem.com209.54.180.3Port 443	SHA1 322928465d67…

Application	Risk	File	Size	Destination	Hash
Unknown	LOW Score: 40	application/ocsp-response	471 B	dsum.casalemedia.com104.122.81.53Port 443	SHA1 b65d948a3029…
Unknown	LOW Score: 40	application/ocsp-response	1.4 KB	acdn.adnxs.com151.101.141.108Port 443	SHA1 be8eba959317…
Unknown	LOW Score: 40	application/ocsp-response	471 B	px.ads.linkedin.com13.107.42.14Port 443	SHA1 aee8808f374d…
Unknown	LOW Score: 40	application/ocsp-response	1.7 KB	c.bing.com204.79.197.200Port 443	SHA1 197a54f4f533…
Unknown	LOW Score: 40	application/ocsp-response	1.4 KB	sync-tm.everesttech.net199.232.82.49Port 443	SHA1 a68dc8dfc889…
Unknown	LOW Score: 40	application/ocsp-response	1.4 KB	sync-tm.everesttech.net199.232.82.49Port 443	SHA1 a68dc8dfc889…
Unknown	LOW Score: 40	application/ocsp-response	471 B	um.simpli.fi169.50.137.184Port 443	SHA1 188b539c61ad…
Unknown	LOW Score: 40	application/ocsp-response	471 B	um.simpli.fi169.50.137.184Port 443	SHA1 188b539c61ad…
Unknown	LOW Score: 40	application/ocsp-response	471 B	um.simpli.fi169.50.137.184Port 443	SHA1 188b539c61ad…
Unknown	LOW Score: 40	application/ocsp-response	313 B	sync.technoratimedia.com193.122.130.38Port 443	SHA1 288f96863df7…
Unknown	LOW Score: 40	application/ocsp-response	313 B	sync.technoratimedia.com193.122.130.38Port 443	SHA1 7d4b9986836f…
Unknown	Moderate Score: 40		23 B	159.138.146.100Port 80	SHA1 d79ea59c77fa…
Unknown	Moderate Score: 40		120 B	159.138.146.100Port 80	SHA1 7da885345123…

Application	Risk	File	Size	Destination	Hash
Unknown	Moderate Score: 40		253 B	159.138.146.100Port 80	SHA1 38e25e656b46…
Unknown	Moderate Score: 40		33 B	159.138.146.100Port 80	SHA1 13e5e555d1c3…
Unknown	Moderate Score: 40		8 B	159.138.146.100Port 80	SHA1 a99de7f06b22…
Unknown	Moderate Score: 40		4 B	159.138.146.100Port 80	SHA1 f32cc36a3474…
Unknown	Moderate Score: 40		23 B	159.138.146.100Port 80	SHA1 cfb0e775eb11…
Unknown	Moderate Score: 40		120 B	159.138.146.100Port 80	SHA1 c007d2d587ff…
Unknown	Moderate Score: 40		253 B	159.138.146.100Port 80	SHA1 69a905e814d9…
Unknown	Moderate Score: 40		33 B	159.138.146.100Port 80	SHA1 1d3a6fe7930d…
Unknown	Moderate Score: 40		8 B	159.138.146.100Port 80	SHA1 731c0d405802…
Unknown	Moderate Score: 40		4 B	159.138.146.100Port 80	SHA1 f32cc36a3474…

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
Moderate Score: 55	match.prod.bidr.io 54.236.195.76:443	*.match.prod.bidr.ioIssuer: Amazon	TLS 1.2	• +30 SNI 'match.prod.bidr.io' != CN '*.match.prod.bidr.io' (domain fronting indicator) • +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
Moderate Score: 55	rtb.adentifi.com 54.174.34.153:443	adentifi.comIssuer: Amazon	TLS 1.2	• +30 SNI 'rtb.adentifi.com' != CN 'adentifi.com' (domain fronting indicator) • +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
Moderate Score: 50	hbopenbid.pubmatic.com 103.231.98.193:443	*.pubmatic.comIssuer: DigiCert Baltimore TLS RSA SHA	TLS 1.2	• +40 Self-signed certificate detected • +10 Unknown application with certificate anomalies
Moderate Score: 50	c.bing.com 204.79.197.200:443	www.bing.comIssuer: Microsoft RSA TLS CA 01	TLS 1.2	• +30 SNI 'c.bing.com' != CN 'www.bing.com' (domain fronting indicator) • +10 Validation error: unable to get local issuer certificate • +10 Unknown application with certificate anomalies
Moderate Score: 50	image6.pubmatic.com 103.231.98.196:443	*.pubmatic.comIssuer: DigiCert Baltimore TLS RSA SHA	TLS 1.2	• +40 Self-signed certificate detected • +10 Unknown application with certificate anomalies

Evaluation	Server / Port	Certificate	TLS	Technical Observations
Moderate Score: 50	simage2.pubmatic.com 103.231.98.194:443	*.pubmatic.comIssuer: DigiCert Baltimore TLS RSA SHA	TLS 1.2	• +40 Self-signed certificate detected • +10 Unknown application with certificate anomalies
Moderate Score: 50	image4.pubmatic.com 103.231.98.195:443	*.pubmatic.comIssuer: DigiCert Baltimore TLS RSA SHA	TLS 1.2	• +40 Self-signed certificate detected • +10 Unknown application with certificate anomalies
Moderate Score: 50	simage4.pubmatic.com 67.199.150.85:443	*.pubmatic.comIssuer: DigiCert Baltimore TLS RSA SHA	TLS 1.2	• +40 Self-signed certificate detected • +10 Unknown application with certificate anomalies
Moderate Score: 45	cdn.ampproject.org 142.250.200.193:443	misc-sni.google.comIssuer: GTS CA 1C3	TLS 1.2	• +30 SNI 'cdn.ampproject.org' != CN 'misc-sni.google.com' (domain fronting indicator) • +5 Free certificate (CN=GTS CA 1C3,O=Google Trust Services LLC,C=US) • +10 Unknown application with certificate anomalies
Moderate Score: 45	edge.api.brightcove.com 151.101.142.27:443	*.adapter.ooyala.comIssuer: GlobalSign Atlas R3 DV TLS CA	TLS 1.2	• +30 SNI 'edge.api.brightcove.com' != CN '*.adapter.ooyala.com' (domain fronting indicator) • +5 Free certificate (CN=GlobalSign Atlas R3 DV TLS CA 2020,O=GlobalSign nv-sa,C=BE) • +10 Unknown application with certificate anomalies

Evaluation	Server / Port	Certificate	TLS	Technical Observations
Moderate Score: 45	id5-sync.com 51.89.21.5:443	*.id5-sync.comIssuer: R3	TLS 1.2	• +30 SNI 'id5-sync.com' != CN '*.id5-sync.com' (domain fronting indicator) • +5 Free certificate (CN=R3,O=Let's Encrypt,C=US) • +10 Unknown application with certificate anomalies
Moderate Score: 45	bttrack.com 192.132.33.46:443	*.bttrack.comIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +30 SNI 'bttrack.com' != CN '*.bttrack.com' (domain fronting indicator) • +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
Moderate Score: 45	cm.adgrx.com 63.251.232.170:443	public1.adgear.comIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +30 SNI 'cm.adgrx.com' != CN 'public1.adgear.com' (domain fronting indicator) • +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
Moderate Score: 45	62ea30a39dede4f6d44ac2895910510 76c294526.cws.conviva.com 199.127.194.97:443	cws.conviva.comIssuer: Sectigo RSA Organization Valid	TLS 1.2	• +30 SNI '62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com' != CN 'cws.conviva.com' (domain fronting indicator) • +5 Free certificate (CN=Sectigo RSA Organization Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
Moderate Score: 45	62ea30a39dede4f6d44ac28959	cws.conviva.comIssuer: Sectigo RSA Organization Valid	TLS 1.2	• +30 SNI '62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com' != CN 'cws.conviva.com' (domain fronting indicator)

Evaluation	Server / Port	Certificate	TLS	Technical Observations
	10510 76c29 4526.c ws.con viva.co m 199.12 7.193.1 08:443			• +5 Free certificate (CN=Sectigo RSA Organization Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
Moderate Score: 40	ae.link edin.c om 144.2.1 5.5:443	us.linkedin.comIssuer: DigiCert SHA2 Secure Server CA	TLS 1.2	• +30 SNI 'ae.linkedin.com' != CN 'us.linkedin.com' (domain fronting indicator) • +10 Unknown application with certificate anomalies
Moderate Score: 40	js-sec.ind exww. com 104.12 2.81.53 :443	san.casalemedia.comIssuer: GeoTrust RSA CA 2018	TLS 1.2	• +30 SNI 'js-sec.indexww.com' != CN 'san.casalemedia.com' (domain fronting indicator) • +10 Unknown application with certificate anomalies
Moderate Score: 40	htlb.ca salem edia.c om 2.21.11 1.28:44 3	san.casalemedia.comIssuer: GeoTrust RSA CA 2018	TLS 1.2	• +30 SNI 'htlb.casalemedia.com' != CN 'san.casalemedia.com' (domain fronting indicator) • +10 Unknown application with certificate anomalies
Moderate Score: 40	acdn.a dnxs.c om 151.10 1.141.1 08:443	cdn.adnxs.comIssuer: GlobalSign Organization Valida	TLS 1.2	• +30 SNI 'acdn.adnxs.com' != CN 'cdn.adnxs.com' (domain fronting indicator) • +10 Unknown application with certificate anomalies
Moderate Score: 40	c1.adf orm.net	track.adform.netIssuer: DigiCert TLS RSA SHA256 2020 C	TLS 1.2	• +30 SNI 'c1.adform.net' != CN 'track.adform.net' (domain fronting indicator)

Evaluation	Server / Port	Certificate	TLS	Technical Observations
	185.84.60.20:443			• +10 Unknown application with certificate anomalies
Moderate Score: 35	inbox.google.com 172.217.171.197:443	mail.google.comIssuer: GTS CA 1C3	TLS 1.2	• +30 SNI 'inbox.google.com' != CN 'mail.google.com' (domain fronting indicator) • +5 Free certificate (CN=GTS CA 1C3,O=Google Trust Services LLC,C=US)
LOW Score: 25	ads.yieldmo.com 54.254.235.164:443	*.yieldmo.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	btlr.sharethrough.com 54.255.100.22:443	*.sharethrough.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	c.deployads.com 52.205.117.34:443	*.deployads.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies

Evaluation	Server / Port	Certificate	TLS	Technical Observations
LOW Score: 25	aax-eu.amazon-adsystem.com 54.239.38.253:443	aax-eu.amazon-adsystem.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	match.sharethrough.com 52.77.1.3:443	*.sharethrough.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	s.amazon-adsystem.com 209.54.180.3:443	s.amazon-adsystem.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	id.sharedid.org 52.10.19.115:443	id.sharedid.orgIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	pm.w55c.net 13.228.74.15:443	*.w55c.netIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25		*.gumgum.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US

Evaluation	Server / Port	Certificate	TLS	Technical Observations
	rtb.gumgum.com 54.178.144.187:443			• +10 Unknown application with certificate anomalies
LOW Score: 25	c.deployads.com 54.220.62.216:443	*.deployads.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	btlr.sharethrough.com 54.251.155.125:443	*.sharethrough.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	ads.yieldmo.com 3.1.139.153:443	*.yieldmo.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 25	btlr.sharethrough.com 52.220.250.98:443	*.sharethrough.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US • +10 Unknown application with certificate anomalies
LOW Score: 15	push.mobilefonex.com	push.mobilefonex.comIssuer: R3	TLS 1.2	• +5 Free certificate (CN=R3,O=Let's Encrypt,C=US) • +10 Unknown application with certificate anomalies

Evaluation	Server / Port	Certificate	TLS	Technical Observations
	119.8.47.97:443			
LOW Score: 15	resolver.msg.global.xiaomi.net 47.241.56.51:443	resolver.msg.global.xiaomi.netIssuer: TrustAsia TLS RSA CA	TLS 1.2	• +5 Free certificate (CN=TrustAsia TLS RSA CA,OU=Domain Validated SSL,O=TrustAsia Technologies\\, Inc.,C=CN) • +10 Unknown application with certificate anomalies
LOW Score: 15	pro.ip-api.com 208.95.112.2:443	*.ip-api.comIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
LOW Score: 15	vjs.zencdn.net 151.101.142.217:443	vjs.zencdn.netIssuer: GlobalSign Atlas R3 DV TLS CA	TLS 1.2	• +5 Free certificate (CN=GlobalSign Atlas R3 DV TLS CA H2 2021,O=GlobalSign nv-sa,C=BE) • +10 Unknown application with certificate anomalies
LOW Score: 15	tlx.3lift.com 54.93.106.38:443	*.3lift.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US
LOW Score: 15	sync.inmobi.com 20.72.149.136:443	sync.inmobi.comIssuer: Sectigo RSA Organization Valid	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Organization Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies

Evaluation	Server / Port	Certificate	TLS	Technical Observations
LOW Score: 15	eb2.3lift.com 13.248.245.213:443	*.3lift.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US
LOW Score: 15	sync.1rx.io 74.118.186.45:443	*.1rx.ioIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
LOW Score: 15	data.adsrvr.org 15.197.193.217:443	*.adsrvr.orgIssuer: GlobalSign GCC R3 DV TLS CA 20	TLS 1.2	• +5 Free certificate (CN=GlobalSign GCC R3 DV TLS CA 2020,O=GlobalSign nv-sa,C=BE) • +10 Unknown application with certificate anomalies
LOW Score: 15	p.rfihub.com 198.8.71.128:443	*.rfihub.comIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
LOW Score: 15	x.bidswitch.net 3.121.19.101:443	*.bidswitch.netIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
LOW Score: 15	sync-tm.everesttech.net 199.232.82.49:443	*.everesttech.netIssuer: GlobalSign Atlas R3 DV TLS CA	TLS 1.2	• +5 Free certificate (CN=GlobalSign Atlas R3 DV TLS CA 2022 Q1,O=GlobalSign nv-sa,C=BE) • +10 Unknown application with certificate anomalies

Evaluation	Server / Port	Certificate	TLS	Technical Observations
LOW Score: 15	core.iprom.net 195.5.165.20:443	*.iprom.netIssuer: R3	TLS 1.2	• +5 Free certificate (CN=R3,O=Let's Encrypt,C=US) • +10 Unknown application with certificate anomalies
LOW Score: 15	dps.jp.cinarra.com 18.179.236.28:443	*.jp.cinarra.comIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
LOW Score: 15	sync-dsp.ad-m.asia 202.131.200.84:443	sync-dsp.ad-m.asiaIssuer: GlobalSign GCC R3 DV TLS CA 20	TLS 1.2	• +5 Free certificate (CN=GlobalSign GCC R3 DV TLS CA 2020,O=GlobalSign nv-sa,C=BE) • +10 Unknown application with certificate anomalies
LOW Score: 15	ads.creative-serving.com 3.120.18.167:443	*.creative-serving.comIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies
LOW Score: 15	tlx.3lift.com 3.124.152.204:443	*.3lift.comIssuer: Amazon	TLS 1.2	• +15 Unknown/untrusted issuer: CN=Amazon,OU=Server CA 1B,O=Amazon,C=US
LOW Score: 15	x.bidswitch.net 18.185.222.19:443	*.bidswitch.netIssuer: Sectigo RSA Domain Validation	TLS 1.2	• +5 Free certificate (CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB) • +10 Unknown application with certificate anomalies

Evaluation	Server / Port	Certificate	TLS	Technical Observations
LOW Score: 10	mtalk.google.com 173.194.76.188:5228	Unknown	TLS 1.3	• +10 TLS on high port 5228
LOW Score: 10	mtalk.google.com 108.177.15.188:5228	Unknown	TLS 1.3	• +10 TLS on high port 5228
LOW Score: 10	mtalk.google.com 74.125.206.188:5228	Unknown	TLS 1.3	• +10 TLS on high port 5228
LOW Score: 10	mtalk.google.com 64.233.184.188:5228	Unknown	TLS 1.3	• +10 TLS on high port 5228
LOW Score: 5	ssl.gstatic.com 142.251.37.227:443	*.gstatic.comIssuer: GTS CA 1C3	TLS 1.2	• +5 Free certificate (CN=GTS CA 1C3,O=Google Trust Services LLC,C=US)
LOW Score: 5	mab.chartbeat.com 151.101.2.202:443	*.chartbeat.comIssuer: GlobalSign Atlas R3 DV TLS CA	TLS 1.2	• +5 Free certificate (CN=GlobalSign Atlas R3 DV TLS CA 2022 Q1,O=GlobalSign nv-sa,C=BE)

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: 1 total
- High priority: 1
- Medium priority: 0
- Low priority: 0

Critical threat detected: 1 critical finding, active C2 communication suspected.

10.215.173.2:53

LOW (0% conf)

Enrichment: ASN: Private | Bytes: ↑10.3 KB ↓26.3 KB

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

Observation: Connessione TCP/dns. verso 10.215.173.2:53. con 10565 bytes inviati e 26945 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

62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com (199.127.194.97:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS11483 | Bytes: ↑6.8 KB ↓11.8 KB

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

Observation: Connessione TCP/ssl. verso 62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com (199.127.194.97:443). con 6978 bytes inviati e 12127 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

62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com (199.127.193.108:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS11483 | Bytes: ↑4.0 KB ↓21.2 KB

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

Observation: Connessione TCP/ssl. verso 62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com (199.127.193.108:443). con 4144 bytes inviati e 21712 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

a.pub.network (104.26.0.139:443) MEDIUM (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑1.3 KB ↓353.1 KB

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

Observation: Connessione TCP/ssl. verso a.pub.network (104.26.0.139:443). con 1289 bytes inviati e 361536 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

a.tribalfusion.com (104.18.13.5:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑4.4 KB ↓8.6 KB

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

Observation: Connessione TCP/ssl. verso a.tribalfusion.com (104.18.13.5:443). con 4547 bytes inviati e 8856 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

a.tribalfusion.com (104.18.13.5:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑4.4 KB ↓8.6 KB

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

Observation: Connessione TCP/tls. verso a.tribalfusion.com (104.18.13.5:443). con 4547 bytes inviati e 8856 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

aax-eu.amazon-adsystem.com (54.239.38.253:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑9.4 KB ↓16.0 KB

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

Observation: Connessione TCP/ssl. verso aax-eu.amazon-adsystem.com (54.239.38.253:443). con 9592 bytes inviati e 16342 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

acdn.adnxs.com (151.101.141.108:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS54113 | Bytes: ↑1.2 KB ↓22.8 KB

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

Observation: Connessione TCP/ssl. verso acdn.adnxs.com (151.101.141.108:443). con 1252 bytes inviati e 23375 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

ad.doubleclick.net (142.251.37.198:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑1.7 KB ↓10.8 KB

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

Observation: Connessione TCP/ssl. verso ad.doubleclick.net (142.251.37.198:443). con 1711 bytes inviati e 11057 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

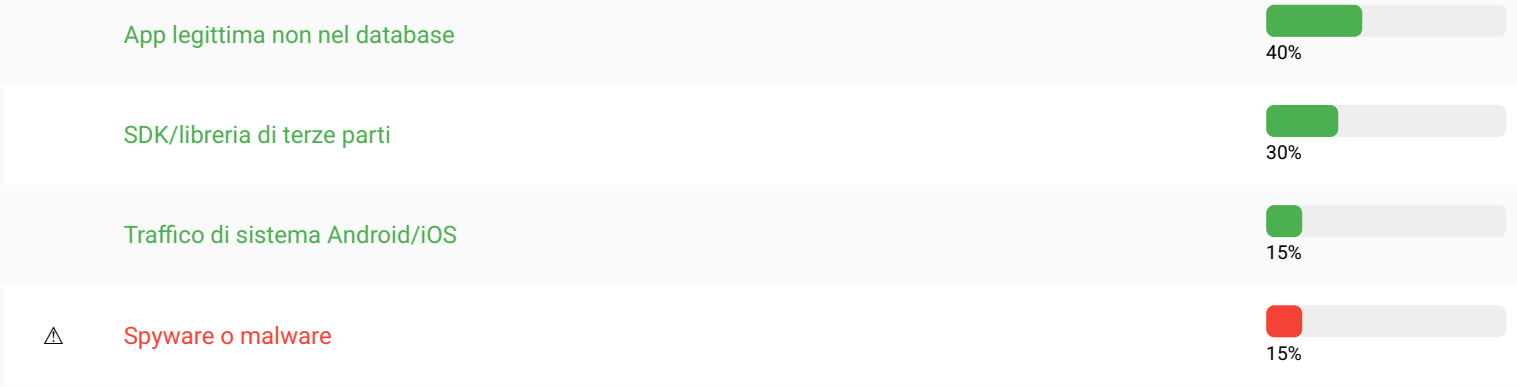
ad.turn.com (46.228.164.11:443) LOW (33% conf)

Enrichment: Geo: United Kingdom | ASN: AS56396 | Bytes: ↑2.4 KB ↓15.2 KB

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

Observation: Connessione TCP/ssl. verso ad.turn.com (46.228.164.11:443). con 2430 bytes inviati e 15522 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

ads.creative-serving.com (3.120.18.167:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑4.3 KB ↓20.5 KB

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

Observation: Connessione TCP/ssl. verso ads.creative-serving.com (3.120.18.167:443). con 4407 bytes inviati e 21021 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

ads.playground.xyz (34.102.253.54:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑1.7 KB ↓11.1 KB

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

Observation: Connessione TCP/ssl. verso ads.playground.xyz (34.102.253.54:443). con 1765 bytes inviati e 11345 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

ads.pubmatic.com (104.122.80.250:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS8529 | Bytes: ↑3.0 KB ↓30.3 KB

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

Observation: Connessione TCP/ssl. verso ads.pubmatic.com (104.122.80.250:443). con 3107 bytes inviati e 31026 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

ads.yieldmo.com (54.254.235.164:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑6.5 KB ↓17.4 KB

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

Observation: Connessione TCP/ssl. verso ads.yieldmo.com (54.254.235.164:443). con 6615 bytes inviati e 17791 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

ads.yieldmo.com (3.1.139.153:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑3.0 KB ↓11.4 KB

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

Observation: Connessione TCP/ssl. verso ads.yieldmo.com (3.1.139.153:443). con 3082 bytes inviati e 11672 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

ae.linkedin.com (144.2.15.5:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS14413 | Bytes: ↑1.7 KB ↓14.1 KB

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

Observation: Connessione TCP/ssl. verso ae.linkedin.com (144.2.15.5:443). con 1779 bytes inviati e 14423 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

app.chat.global.xiaomi.net (161.117.185.166:5222) LOW (28% conf)

Enrichment: Geo: Singapore | ASN: AS45102 | Bytes: ↑1.1 KB ↓171 B

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

Observation: Connessione TCP/xmpp. verso app.chat.global.xiaomi.net (161.117.185.166:5222). con 1096 bytes inviati e 171 bytes ricevuti.

Alternative Hypotheses:

Cloud backup (Google Drive, iCloud, OneDrive) — 35%

Videochiamata con camera attiva — 25%

Condivisione file (WhatsApp, Telegram) — 20%

Telemetria/Analytics legittima — 10%

⚠ Esfiltrazione dati 10%

Conclusion: Comportamento probabilmente legittimo: Cloud backup (Google Drive, iCloud, OneDrive)

app.chat.global.xiaomi.net (47.241.35.73:5222) LOW (28% conf)

Enrichment: Geo: United States | ASN: AS45102 | Bytes: ↑1.1 KB ↓171 B

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

Observation: Connessione TCP/xmpp. verso app.chat.global.xiaomi.net (47.241.35.73:5222). con 1101 bytes inviati e 171 bytes ricevuti.

Alternative Hypotheses:

Cloud backup (Google Drive, iCloud, OneDrive) 35%

Videochiamata con camera attiva 25%

Condivisione file (WhatsApp, Telegram) 20%

Telemetria/Analytics legittima 10%

⚠ Esfiltrazione dati 10%

Conclusion: Comportamento probabilmente legittimo: Cloud backup (Google Drive, iCloud, OneDrive)

app.chat.global.xiaomi.net (47.241.72.88:5222) LOW (28% conf)

Enrichment: Geo: United States | ASN: AS45102 | Bytes: ↑1.1 KB ↓183 B

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

Observation: Connessione TCP/xmpp. verso app.chat.global.xiaomi.net (47.241.72.88:5222). con 1105 bytes inviati e 183 bytes ricevuti.

Alternative Hypotheses:

	Cloud backup (Google Drive, iCloud, OneDrive)	35%
	Videochiamata con camera attiva	25%
	Condivisione file (WhatsApp, Telegram)	20%
	Telemetria/Analytics legittima	10%
⚠	Esfiltrazione dati	10%

Conclusion: Comportamento probabilmente legittimo: Cloud backup (Google Drive, iCloud, OneDrive)

b1sync.zemanta.com (50.31.142.63:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS22075 | Bytes: ↑3.6 KB ↓10.6 KB

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

Observation: Connessione TCP/ssl. verso b1sync.zemanta.com (50.31.142.63:443). con 3706 bytes inviati e 10858 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

bam.nr-data.net (162.247.242.21:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS23467 | Bytes: ↑33.0 KB ↓11.1 KB

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

Observation: Connessione TCP/ssl. verso bam.nr-data.net (162.247.242.21:443). con 33831 bytes inviati e 11385 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

	Cloud backup (Google Drive, iCloud, OneDrive)	35%

Videochiamata con camera attiva — 25%

Condivisione file (WhatsApp, Telegram) — 20%

Telemetria/Analytics legittima — 10%

⚠ Esfiltrazione dati — 10%

Conclusion: Comportamento probabilmente legittimo: Cloud backup (Google Drive, iCloud, OneDrive)

bidder.criteo.com (178.250.2.131:443) LOW (33% conf)

Enrichment: Geo: France | ASN: ASNA | Bytes: ↑11.4 KB ↓23.7 KB

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

Observation: Connessione TCP/ssl. verso bidder.criteo.com (178.250.2.131:443). con 11702 bytes inviati e 24220 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

bidder.criteo.com (178.250.2.131:443) LOW (33% conf)

Enrichment: Geo: France | ASN: ASNA | Bytes: ↑11.4 KB ↓23.7 KB

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

Observation: Connessione TCP/tls. verso bidder.criteo.com (178.250.2.131:443). con 11702 bytes inviati e 24220 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

btloader.com (172.67.70.134:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑990 B ↓33.4 KB

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

Observation: Connessione TCP/ssl. verso btloader.com (172.67.70.134:443). con 990 bytes inviati e 34167 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

btlr.sharethrough.com (54.255.100.22:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑5.0 KB ↓28.8 KB

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

Observation: Connessione TCP/ssl. verso btlr.sharethrough.com (54.255.100.22:443). con 5081 bytes inviati e 29462 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

btlr.sharethrough.com (54.255.100.22:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑5.0 KB ↓28.8 KB

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

Observation: Connessione TCP/tls. verso btlr.sharethrough.com (54.255.100.22:443). con 5081 bytes inviati e 29462 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

btlr.sharethrough.com (54.251.155.125:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑4.2 KB ↓17.7 KB

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

Observation: Connessione TCP/tls. verso btlr.sharethrough.com (54.251.155.125:443). con 4287 bytes inviati e 18083 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

btlr.sharethrough.com (54.251.155.125:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑4.2 KB ↓17.7 KB

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

Observation: Connessione TCP/ssl. verso btlr.sharethrough.com (54.251.155.125:443). con 4287 bytes inviati e 18083 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

btlr.sharethrough.com (52.220.250.98:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑1.6 KB ↓10.5 KB

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

Observation: Connessione TCP/tls. verso btlr.sharethrough.com (52.220.250.98:443). con 1656 bytes inviati e 10780 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

btlr.sharethrough.com (52.220.250.98:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑1.6 KB ↓10.5 KB

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

Observation: Connessione TCP/ssl. verso btlr.sharethrough.com (52.220.250.98:443). con 1656 bytes inviati e 10780 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

bttrack.com (192.132.33.46:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS18568 | Bytes: ↑2.3 KB ↓9.9 KB

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

Observation: Connessione TCP/ssl. verso bttrack.com (192.132.33.46:443). con 2326 bytes inviati e 10108 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

c.amazon-adsystem.com (52.222.142.111:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑7.0 KB ↓71.9 KB

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

Observation: Connessione TCP/ssl. verso c.amazon-adsystem.com (52.222.142.111:443). con 7203 bytes inviati e 73594 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

c.amazon-adsystem.com (99.86.116.84:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: ASNA | Bytes: ↑3.9 KB ↓7.9 KB

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

Observation: Connessione TCP/ssl. verso c.amazon-adsystem.com (99.86.116.84:443). con 4039 bytes inviati e 8050 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

c.deployads.com (52.205.117.34:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS14618 | Bytes: ↑10.4 KB ↓30.8 KB

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

Observation: Connessione TCP/ssl. verso c.deployads.com (52.205.117.34:443). con 10609 bytes inviati e 31491 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

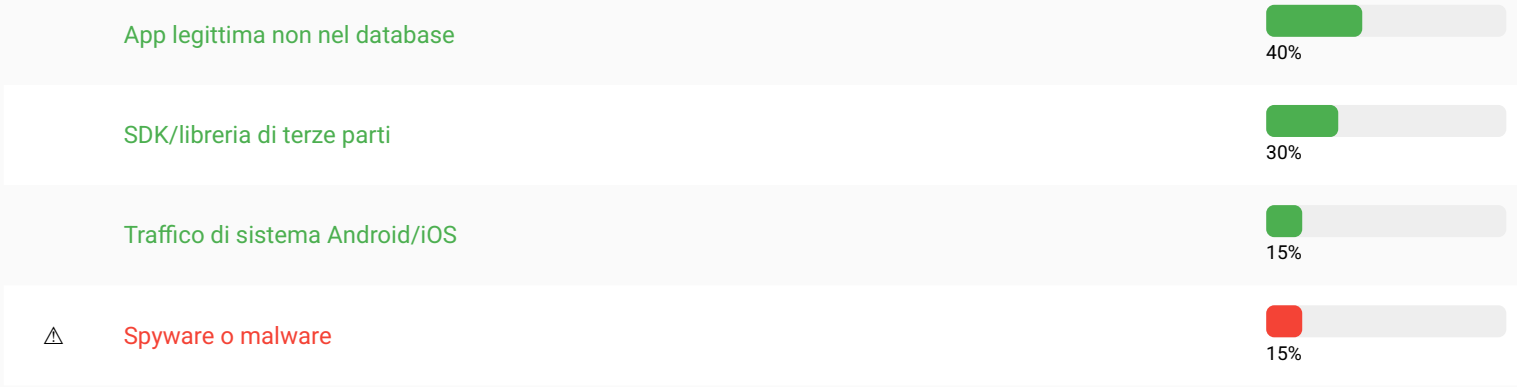
c.deploads.com (54.220.62.216:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑6.1 KB ↓18.0 KB

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

Observation: Connessione TCP/ssl. verso c.deploads.com (54.220.62.216:443). con 6263 bytes inviati e 18385 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

c1.adform.net (185.84.60.20:443) LOW (33% conf)

Enrichment: Geo: Denmark | ASN: AS198622 | Bytes: ↑6.2 KB ↓21.7 KB

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

Observation: Connessione TCP/tls. verso c1.adform.net (185.84.60.20:443). con 6372 bytes inviati e 22250 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

c1.adform.net (185.84.60.20:443) LOW (33% conf)

Enrichment: Geo: Denmark | ASN: AS198622 | Bytes: ↑6.2 KB ↓21.7 KB

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

Observation: Connessione TCP/ssl. verso c1.adform.net (185.84.60.20:443). con 6372 bytes inviati e 22250 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

casale-match.dotomi.com (89.207.16.140:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS41041 | Bytes: ↑3.0 KB ↓12.0 KB

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

Observation: Connessione TCP/tls. verso casale-match.dotomi.com (89.207.16.140:443). con 3113 bytes inviati e 12331 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

casale-match.dotomi.com (89.207.16.140:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS41041 | Bytes: ↑3.0 KB ↓12.0 KB

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

Observation: Connessione TCP/ssl. verso casale-match.dotomi.com (89.207.16.140:443). con 3113 bytes inviati e 12331 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

cdn.ampproject.org (142.250.200.193:443) MEDIUM (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑11.3 KB ↓1.2 MB

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

Observation: Connessione TCP/ssl. verso cdn.ampproject.org (142.250.200.193:443). con 11567 bytes inviati e 1294560 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

cdn.cookielaw.org (104.16.148.64:443) MEDIUM (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑3.7 KB ↓164.2 KB

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

Observation: Connessione TCP/ssl. verso cdn.cookielaw.org (104.16.148.64:443). con 3823 bytes inviati e 168164 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

cdn.cookielaw.org (104.16.148.64:443)

MEDIUM (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑3.7 KB ↓164.2 KB

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

Observation: Connessione TCP/tls. verso cdn.cookielaw.org (104.16.148.64:443). con 3823 bytes inviati e 168164 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

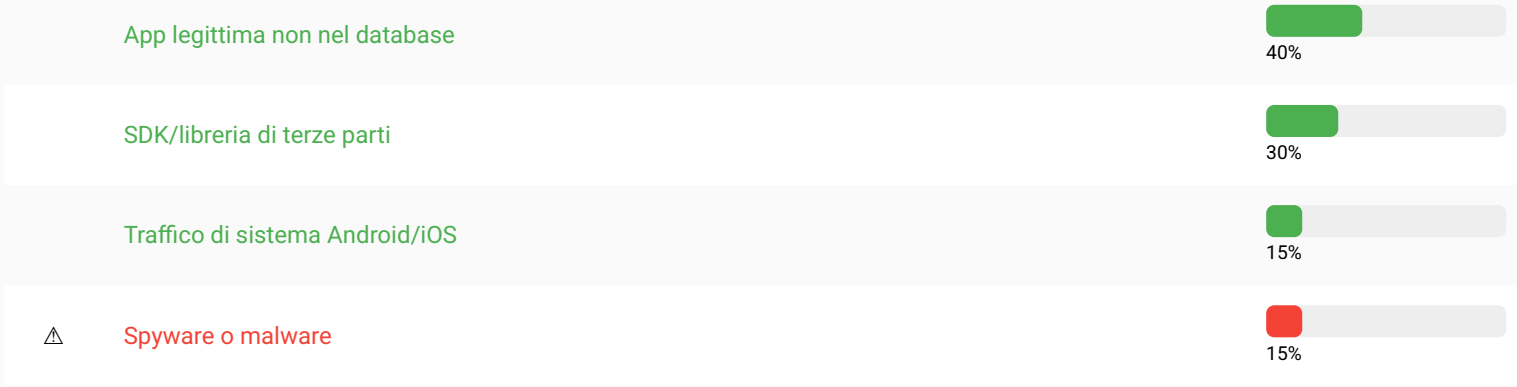
cdn.id5-sync.com (46.105.202.126:443) LOW (33% conf)

Enrichment: Geo: France | ASN: AS16276 | Bytes: ↑1.6 KB ↓20.1 KB

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

Observation: Connessione TCP/ssl. verso cdn.id5-sync.com (46.105.202.126:443). con 1599 bytes inviati e 20558 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

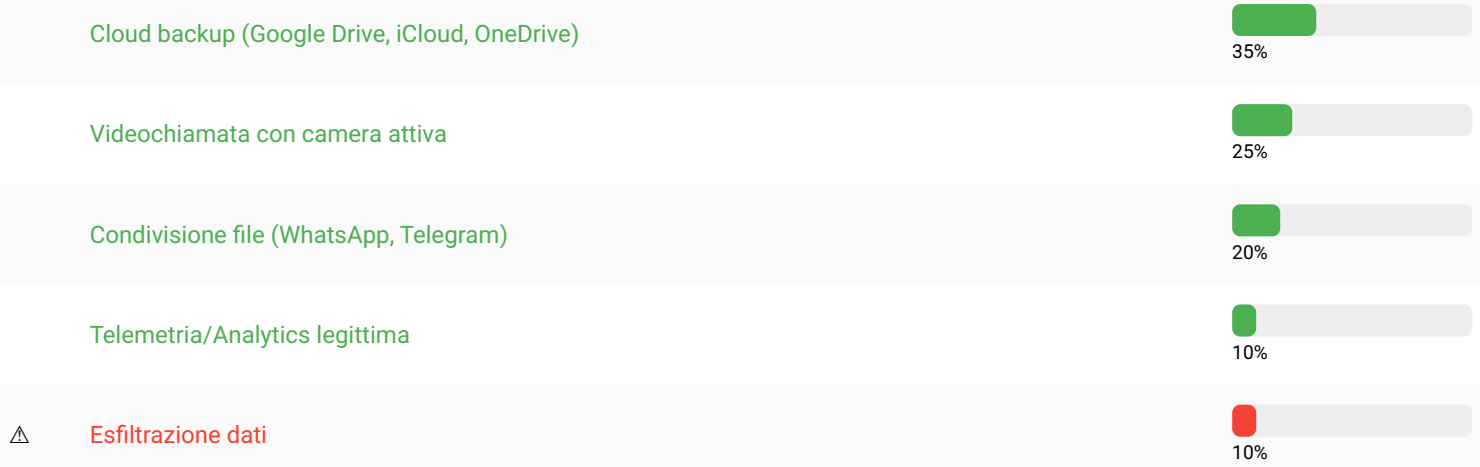
client.mobilefonex.com (159.138.146.100:80) LOW (33% conf)

Enrichment: Geo: Singapore | ASN: AS136907 | Bytes: ↑7.9 KB ↓3.6 KB

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

Observation: Connessione TCP/http. verso client.mobilefonex.com (159.138.146.100:80). con 8082 bytes inviati e 3696 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: Cloud backup (Google Drive, iCloud, OneDrive)

cm.adgrx.com (63.251.232.170:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS32475 | Bytes: ↑1.9 KB ↓13.4 KB

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

Observation: Connessione TCP/ssl. verso cm.adgrx.com (63.251.232.170:443). con 1945 bytes inviati e 13732 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

core.iprom.net (195.5.165.20:443) LOW (33% conf)

Enrichment: Geo: Slovenia | ASN: AS44968 | Bytes: ↑1.9 KB ↓9.6 KB

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

Observation: Connessione TCP/ssl. verso core.iprom.net (195.5.165.20:443). con 1901 bytes inviati e 9786 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

cs.media.net (104.122.80.29:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS8529 | Bytes: ↑2.2 KB ↓10.0 KB

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

Observation: Connessione TCP/tls. verso cs.media.net (104.122.80.29:443). con 2238 bytes inviati e 10287 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

cs.media.net (104.122.80.29:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS8529 | Bytes: ↑2.2 KB ↓10.0 KB

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

Observation: Connessione TCP/ssl. verso cs.media.net (104.122.80.29:443). con 2238 bytes inviati e 10287 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

csync.loopme.me (23.88.75.187:443) LOW (33% conf)

Enrichment: Geo: Germany | ASN: AS24940 | Bytes: ↑1.8 KB ↓9.5 KB

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

Observation: Connessione TCP/ssl. verso csync.loopme.me (23.88.75.187:443). con 1829 bytes inviati e 9770 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

d.pub.network (35.201.71.192:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑39.0 KB ↓47.3 KB

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

Observation: Connessione TCP/ssl. verso d.pub.network (35.201.71.192:443). con 39933 bytes inviati e 48461 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

data.adsrvr.org (15.197.193.217:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑4.4 KB ↓20.6 KB

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

Observation: Connessione TCP/ssl. verso data.adsrvr.org (15.197.193.217:443). con 4511 bytes inviati e 21063 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

dps.jp.cinarra.com (18.179.236.28:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑1.9 KB ↓12.3 KB

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

Observation: Connessione TCP/ssl. verso dps.jp.cinarra.com (18.179.236.28:443). con 1957 bytes inviati e 12577 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

dsportal.aljazeera.net (104.18.26.213:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑8.4 KB ↓6.8 KB

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

Observation: Connessione TCP/ssl. verso dsportal.aljazeera.net (104.18.26.213:443). con 8647 bytes inviati e 6944 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

edge.api.brightcove.com (151.101.142.27:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS54113 | Bytes: ↑1.9 KB ↓13.7 KB

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

Observation: Connessione TCP/ssl. verso edge.api.brightcove.com (151.101.142.27:443). con 1983 bytes inviati e 14076 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

freestar-d.openx.net (35.244.159.8:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑7.5 KB ↓22.7 KB

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

Observation: Connessione TCP/ssl. verso freestar-d.openx.net (35.244.159.8:443). con 7677 bytes inviati e 23223 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

g.whatsapp.net (157.240.195.54:5222) LOW (28% conf)

Enrichment: Geo: United States | ASN: AS32934 | Bytes: ↑2.0 KB ↓1.7 KB

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

Observation: Connessione TCP/xmpp. verso g.whatsapp.net (157.240.195.54:5222). con 2098 bytes inviati e 1724 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

gocm.c.appier.net (139.162.38.30:443) LOW (33% conf)

Enrichment: Geo: Netherlands | ASN: AS63949 | Bytes: ↑1.6 KB ↓10.6 KB

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

Observation: Connessione TCP/ssl. verso gocm.c.appier.net (139.162.38.30:443). con 1688 bytes inviati e 10858 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

googleads.g.doubleclick.net (172.217.18.34:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑18.8 KB ↓77.2 KB

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

Observation: Connessione TCP/ssl. verso googleads.g.doubleclick.net (172.217.18.34:443). con 19200 bytes inviati e 79050 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

googleads.g.doubleclick.net (172.217.18.34:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑18.8 KB ↓77.2 KB

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

Observation: Connessione TCP/tls. verso googleads.g.doubleclick.net (172.217.18.34:443). con 19200 bytes inviati e 79050 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

googleads.g.doubleclick.net (142.250.201.34:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑6.5 KB ↓29.3 KB

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

Observation: Connessione TCP/ssl. verso googleads.g.doubleclick.net (142.250.201.34:443). con 6652 bytes inviati e 29983 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

googleads.g.doubleclick.net (142.251.37.162:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑3.4 KB ↓14.7 KB

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

Observation: Connessione TCP/ssl. verso googleads.g.doubleclick.net (142.251.37.162:443). con 3505 bytes inviati e 15037 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

gu.dyntrk.com (51.81.106.33:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS16276 | Bytes: ↑2.1 KB ↓11.4 KB

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

Observation: Connessione TCP/ssl. verso gu.dyntrk.com (51.81.106.33:443). con 2141 bytes inviati e 11707 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

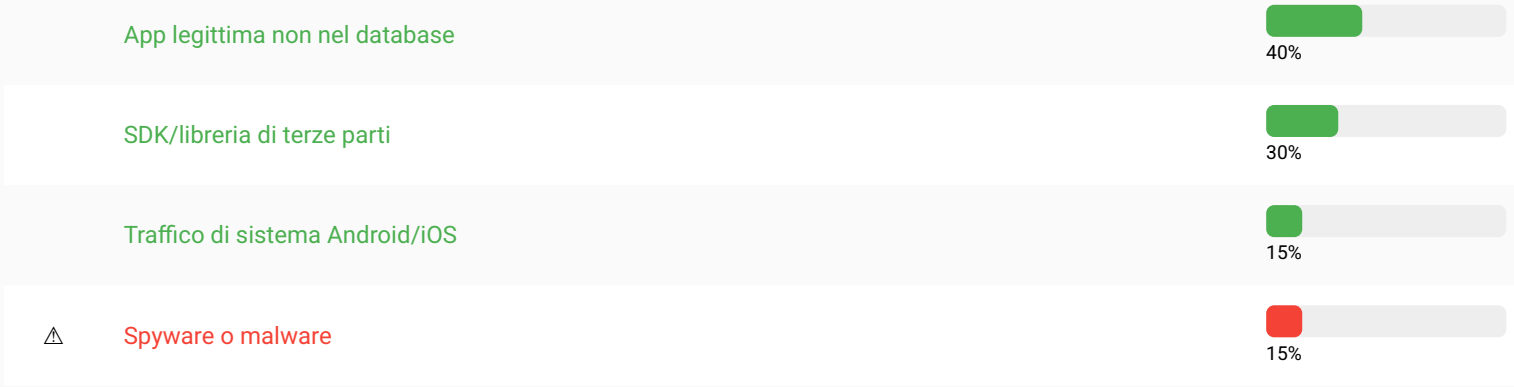
gum.criteo.com (178.250.0.157:443) LOW (33% conf)

Enrichment: Geo: France | ASN: ASNA | Bytes: ↑4.3 KB ↓17.5 KB

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

Observation: Connessione TCP/ssl. verso gum.criteo.com (178.250.0.157:443). con 4403 bytes inviati e 17942 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

hbopenbid.pubmatic.com (103.231.98.193:443) LOW (33% conf)

Enrichment: Geo: Japan | ASN: AS62713 | Bytes: ↑12.8 KB ↓14.1 KB

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

Observation: Connessione TCP/ssl. verso hbopenbid.pubmatic.com (103.231.98.193:443). con 13133 bytes inviati e 14467 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

htlb.casalemedia.com (2.21.111.28:443) LOW (33% conf)

Enrichment: Geo: Netherlands | ASN: AS20940 | Bytes: ↑6.0 KB ↓15.3 KB

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

Observation: Connessione TCP/ssl. verso htlb.casalemedia.com (2.21.111.28:443). con 6177 bytes inviati e 15626 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

htlb.casalemedia.com (2.21.111.28:443) LOW (33% conf)

Enrichment: Geo: Netherlands | ASN: AS20940 | Bytes: ↑6.0 KB ↓15.3 KB

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

Observation: Connessione TCP/tls. verso htlb.casalemedia.com (2.21.111.28:443). con 6177 bytes inviati e 15626 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

ib.adnxs.com (185.33.220.216:443)

LOW (33% conf)

Enrichment: Geo: United States | ASN: AS29990 | Bytes: ↑13.7 KB ↓18.5 KB

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

Observation: Connessione TCP/ssl. verso ib.adnxs.com (185.33.220.216:443). con 14037 bytes inviati e 18927 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

id.rlcdn.com (35.190.60.146:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑3.0 KB ↓21.2 KB

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

Observation: Connessione TCP/ssl. verso id.rlcdn.com (35.190.60.146:443). con 3029 bytes inviati e 21692 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

id.sharedid.org (52.10.19.115:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑1.7 KB ↓11.6 KB

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

Observation: Connessione TCP/ssl. verso id.sharedid.org (52.10.19.115:443). con 1734 bytes inviati e 11851 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

id5-sync.com (51.89.21.5:443) LOW (33% conf)

Enrichment: Geo: France | ASN: AS16276 | Bytes: ↑3.3 KB ↓8.5 KB

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

Observation: Connessione TCP/ssl. verso id5-sync.com (51.89.21.5:443). con 3353 bytes inviati e 8713 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

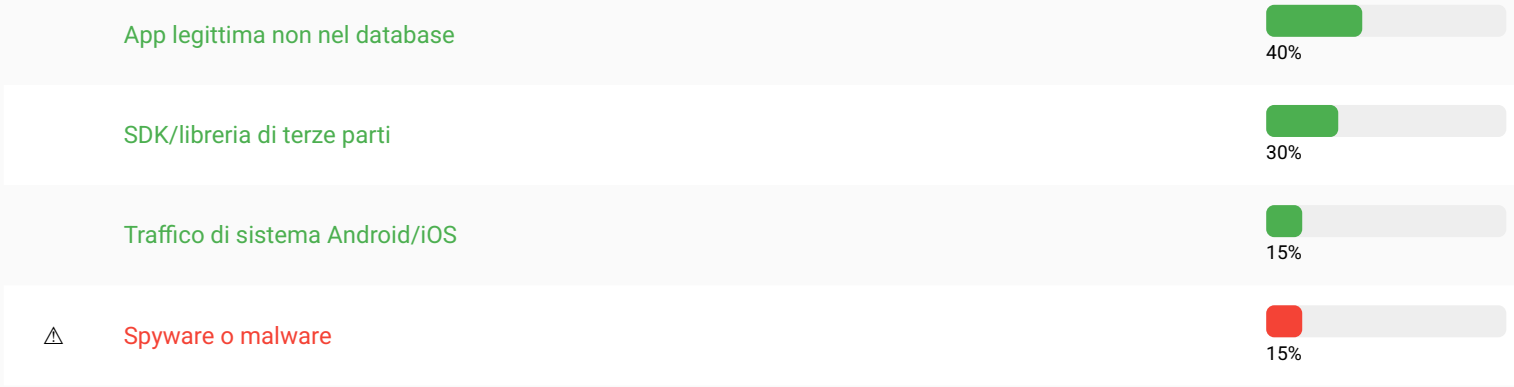
image4.pubmatic.com (103.231.98.195:443) LOW (33% conf)

Enrichment: Geo: Japan | ASN: AS62713 | Bytes: ↑2.6 KB ↓10.6 KB

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

Observation: Connessione TCP/ssl. verso image4.pubmatic.com (103.231.98.195:443). con 2703 bytes inviati e 10806 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

image6.pubmatic.com (103.231.98.196:443) LOW (33% conf)

Enrichment: Geo: Japan | ASN: AS62713 | Bytes: ↑1.6 KB ↓11.4 KB

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

Observation: Connessione TCP/ssl. verso image6.pubmatic.com (103.231.98.196:443). con 1600 bytes inviati e 11709 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

js-agent.newrelic.com (199.232.82.137:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS54113 | Bytes: ↑989 B ↓19.3 KB

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

Observation: Connessione TCP/ssl. verso js-agent.newrelic.com (199.232.82.137:443). con 989 bytes inviati e 19726 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

js-sec.indexww.com (104.122.81.53:443)

MEDIUM (33% conf)

Enrichment: Geo: United States | ASN: AS8529 | Bytes: ↑34.9 KB ↓67.7 KB

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

Observation: Connessione TCP/ssl. verso js-sec.indexww.com (104.122.81.53:443). con 35721 bytes inviati e 69276 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

lh5.googleusercontent.com (172.217.18.225:443)

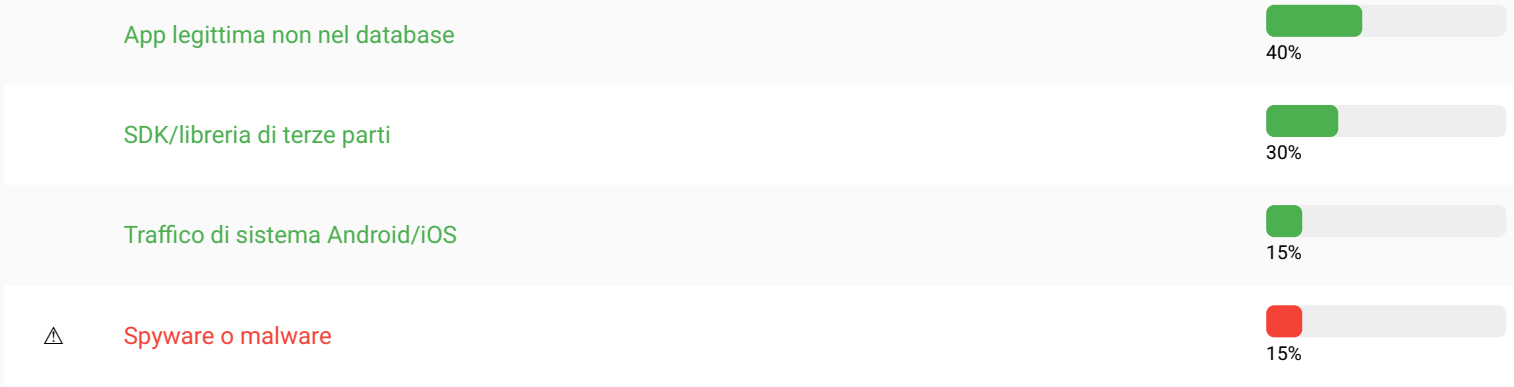
LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑2.6 KB ↓52.7 KB

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

Observation: Connessione TCP/tls. verso lh5.googleusercontent.com (172.217.18.225:443). con 2626 bytes inviati e 54005 bytes ricevuti.

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

lh5.googleusercontent.com (172.217.18.225:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑2.6 KB ↓52.7 KB

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

Observation: Connessione TCP/ssl. verso lh5.googleusercontent.com (172.217.18.225:443). con 2626 bytes inviati e 54005 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

live-hls-web-aja.getaj.net (176.29.114.155:443) MEDIUM (33% conf)

Enrichment: Geo: JO | ASN: AS48832 | Bytes: ↑19.5 KB ↓9.3 MB

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

Observation: Connessione TCP/ssl. verso live-hls-web-aja.getaj.net (176.29.114.155:443). con 19957 bytes inviati e 9703256 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

live-hls-web-aja.getaj.net (176.29.114.155:443) MEDIUM (33% conf)

Enrichment: Geo: JO | ASN: AS48832 | Bytes: ↑19.5 KB ↓9.3 MB

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

Observation: Connessione TCP/tls. verso live-hls-web-aja.getaj.net (176.29.114.155:443). con 19957 bytes inviati e 9703256 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

match.prod.bidr.io (54.236.195.76:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS14618 | Bytes: ↑5.4 KB ↓19.3 KB

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

Observation: Connessione TCP/ssl. verso match.prod.bidr.io (54.236.195.76:443). con 5532 bytes inviati e 19797 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

match.sharethrough.com (52.77.1.3:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑3.0 KB ↓14.1 KB

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

Observation: Connessione TCP/ssl. verso match.sharethrough.com (52.77.1.3:443). con 3041 bytes inviati e 14481 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

metrics.brightcove.com (35.244.232.184:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑23.1 KB ↓21.4 KB

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

Observation: Connessione TCP/ssl. verso metrics.brightcove.com (35.244.232.184:443). con 23662 bytes inviati e 21876 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

metrics.brightcove.com (35.244.232.184:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑23.1 KB ↓21.4 KB

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

Observation: Connessione TCP/tls. verso metrics.brightcove.com (35.244.232.184:443). con 23662 bytes inviati e 21876 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

mtalk.google.com (173.194.76.188:5228) LOW (44% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑959 B ↓850 B

App: Google (44% attribution) | Proto: TCP

Observation: Connessione TCP/ssl. verso mtalk.google.com (173.194.76.188:5228). con 959 bytes inviati e 850 bytes ricevuti. [Encrypted traffic on non-standard port].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: VPN o proxy aziendale

mtalk.google.com (108.177.15.188:5228) LOW (44% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑988 B ↓876 B

App: Google (44% attribution) | Proto: TCP

Observation: Connessione TCP/ssl. verso mtalk.google.com (108.177.15.188:5228). con 988 bytes inviati e 876 bytes ricevuti. [Encrypted traffic on non-standard port].

Alternative Hypotheses:

	VPN o proxy aziendale	30%
	Applicazione gaming o streaming	20%
	Applicazione enterprise interna	20%
	Ambiente di sviluppo/test	15%
⚠	Infrastruttura C2 malevola	15%

Conclusion: Comportamento probabilmente legittimo: VPN o proxy aziendale

mtalk.google.com (74.125.206.188:5228) LOW (44% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑4.7 KB ↓4.1 KB

App: Google (44% attribution) | Proto: TCP

Observation: Connessione TCP/ssl. verso mtalk.google.com (74.125.206.188:5228). con 4810 bytes inviati e 4228 bytes ricevuti. [Encrypted traffic on non-standard port].

Alternative Hypotheses:

	VPN o proxy aziendale	30%
	Applicazione gaming o streaming	20%
	Applicazione enterprise interna	20%
	Ambiente di sviluppo/test	15%
⚠	Infrastruttura C2 malevola	15%

Conclusion: Comportamento probabilmente legittimo: VPN o proxy aziendale

mtalk.google.com (64.233.184.188:5228) LOW (44% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑3.0 KB ↓2.6 KB

App: Google (44% attribution) | Proto: TCP

Observation: Connessione TCP/ssl. verso mtalk.google.com (64.233.184.188:5228). con 3057 bytes inviati e 2630 bytes ricevuti. [Encrypted traffic on non-standard port].

Alternative Hypotheses:

	VPN o proxy aziendale	30%
	Applicazione gaming o streaming	20%

Applicazione enterprise interna 20%

Ambiente di sviluppo/test 15%

⚠ Infrastruttura C2 malevola 15%

Conclusion: Comportamento probabilmente legittimo: VPN o proxy aziendale

nexus.ensighten.com (52.209.177.22:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑2.2 KB ↓32.1 KB

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

Observation: Connessione TCP/ssl. verso nexus.ensighten.com (52.209.177.22:443). con 2284 bytes inviati e 32831 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

p.adsymptotic.com (104.18.98.194:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS13335 | Bytes: ↑2.8 KB ↓7.6 KB

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

Observation: Connessione TCP/ssl. verso p.adsymptotic.com (104.18.98.194:443). con 2853 bytes inviati e 7805 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:

Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

pagead2.googleadservices.com (142.250.200.194:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑9.1 KB ↓5.0 KB

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

Observation: Connessione TCP/ssl. verso pagead2.googleadservices.com (142.250.200.194:443). con 9338 bytes inviati e 5079 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

pagead2.googlesyndication.com (142.251.37.194:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑7.5 KB ↓9.0 KB

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

Observation: Connessione TCP/ssl. verso pagead2.googlesyndication.com (142.251.37.194:443). con 7722 bytes inviati e 9230 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

pagead2.googlesyndication.com (142.250.203.226:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑7.6 KB ↓78.4 KB

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

Observation: Connessione TCP/ssl. verso pagead2.googlesyndication.com (142.250.203.226:443). con 7754 bytes inviati e 80317 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

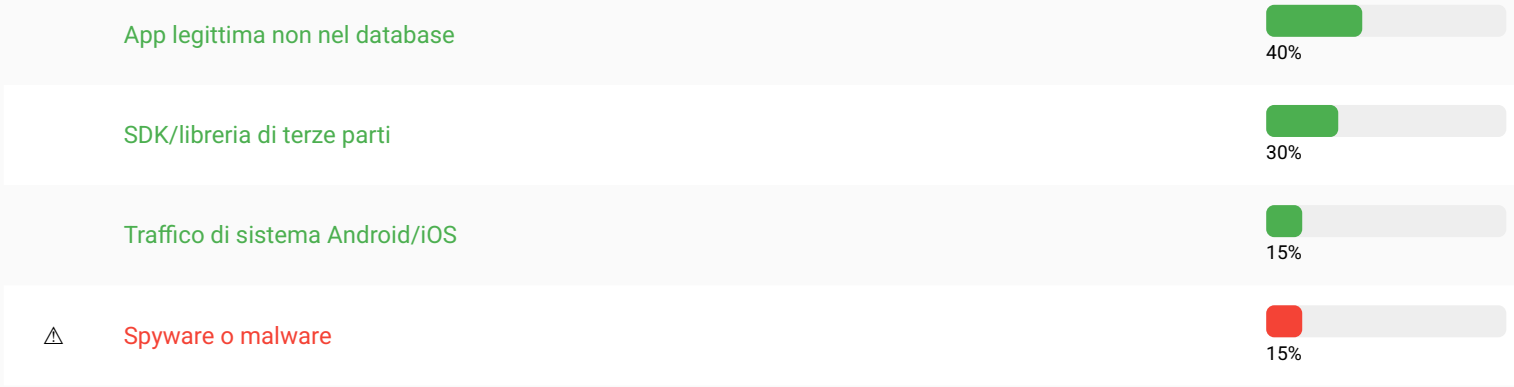
pagead2.googlesyndication.com (172.217.21.2:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑10.7 KB ↓25.3 KB

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

Observation: Connessione TCP/ssl. verso pagead2.googlesyndication.com (172.217.21.2:443). con 10985 bytes inviati e 25936 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

pagead2.googlesyndication.com (172.217.21.2:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑10.7 KB ↓25.3 KB

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

Observation: Connessione TCP/tls. verso pagead2.googlesyndication.com (172.217.21.2:443). con 10985 bytes inviati e 25936 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

pghub.io (35.241.45.217:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑1.6 KB ↓12.1 KB

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

Observation: Connessione TCP/ssl. verso pghub.io (35.241.45.217:443). con 1598 bytes inviati e 12432 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

ping.chartbeat.net (23.20.220.210:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS14618 | Bytes: ↑4.6 KB ↓8.4 KB

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

Observation: Connessione TCP/ssl. verso ping.chartbeat.net (23.20.220.210:443). con 4697 bytes inviati e 8597 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

pippio.com (107.178.254.65:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑2.0 KB ↓11.2 KB

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

Observation: Connessione TCP/ssl. verso pippio.com (107.178.254.65:443). con 2032 bytes inviati e 11460 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

players.brightcove.net (104.122.81.100:443) MEDIUM (33% conf)

Enrichment: Geo: United States | ASN: AS8529 | Bytes: ↑1.0 KB ↓243.6 KB

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

Observation: Connessione TCP/ssl. verso players.brightcove.net (104.122.81.100:443). con 1073 bytes inviati e 249491 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

pm.w55c.net (13.228.74.15:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑4.6 KB ↓18.8 KB

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

Observation: Connessione TCP/ssl. verso pm.w55c.net (13.228.74.15:443). con 4729 bytes inviati e 19262 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

pool.admedo.com (35.210.53.219:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑2.7 KB ↓13.5 KB

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

Observation: Connessione TCP/ssl. verso pool.admedo.com (35.210.53.219:443). con 2802 bytes inviati e 13859 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

pr-bh.ybp.yahoo.com (54.75.169.44:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑2.2 KB ↓12.4 KB

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

Observation: Connessione TCP/tls. verso pr-bh.ybp.yahoo.com (54.75.169.44:443). con 2300 bytes inviati e 12693 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

pr-bh.ybp.yahoo.com (54.75.169.44:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑2.2 KB ↓12.4 KB

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

Observation: Connessione TCP/ssl. verso pr-bh.ybp.yahoo.com (54.75.169.44:443). con 2300 bytes inviati e 12693 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

push.mobilefonex.com (119.8.47.97:443) LOW (33% conf)

Enrichment: Geo: Singapore | ASN: AS136907 | Bytes: ↑6.3 KB ↓32.9 KB

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

Observation: Connessione TCP/ssl. verso push.mobilefonex.com (119.8.47.97:443). con 6439 bytes inviati e 33656 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

rtb.adentifi.com (54.174.34.153:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS14618 | Bytes: ↑2.0 KB ↓11.7 KB

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

Observation: Connessione TCP/ssl. verso rtb.adentifi.com (54.174.34.153:443). con 2028 bytes inviati e 12007 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

rtb.gumgum.com (54.178.144.187:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑1.8 KB ↓11.4 KB

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

Observation: Connessione TCP/ssl. verso rtb.gumgum.com (54.178.144.187:443). con 1861 bytes inviati e 11667 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

rtb.openx.net (35.227.252.103:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑1.9 KB ↓8.3 KB

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

Observation: Connessione TCP/ssl. verso rtb.openx.net (35.227.252.103:443). con 1913 bytes inviati e 8466 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

s.amazon-adsystem.com (209.54.180.3:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑4.9 KB ↓17.1 KB

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

Observation: Connessione TCP/ssl. verso s.amazon-adsystem.com (209.54.180.3:443). con 5032 bytes inviati e 17526 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

sb.scorecardresearch.com (52.222.137.28:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑2.5 KB ↓9.2 KB

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

Observation: Connessione TCP/ssl. verso sb.scorecardresearch.com (52.222.137.28:443). con 2559 bytes inviati e 9451 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

secure.cdn.fastclick.net (23.222.56.60:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS16625 | Bytes: ↑1.6 KB ↓25.3 KB

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

Observation: Connessione TCP/ssl. verso secure.cdn.fastclick.net (23.222.56.60:443). con 1612 bytes inviati e 25929 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

secure.quantserve.com (91.228.74.202:443) LOW (33% conf)

Enrichment: Geo: United Kingdom | ASN: AS16509 27281 | Bytes: ↑2.7 KB ↓18.2 KB

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

Observation: Connessione TCP/ssl. verso secure.quantserve.com (91.228.74.202:443). con 2772 bytes inviati e 18595 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

securepubads.g.doubleclick.net (172.217.171.226:443) MEDIUM (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑31.0 KB ↓240.4 KB

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

Observation: Connessione TCP/ssl. verso securepubads.g.doubleclick.net (172.217.171.226:443). con 31700 bytes inviati e 246158 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

securepubads.g.doubleclick.net (172.217.171.226:443) MEDIUM (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑31.0 KB ↓240.4 KB

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

Observation: Connessione TCP/tls. verso securepubads.g.doubleclick.net (172.217.171.226:443). con 31700 bytes inviati e 246158 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

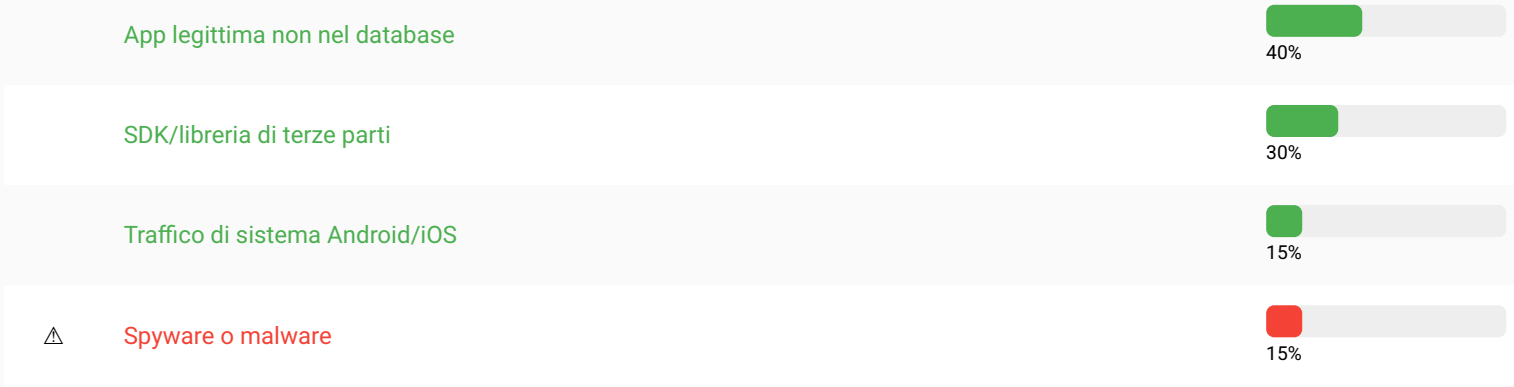
simage2.pubmatic.com (103.231.98.194:443) LOW (33% conf)

Enrichment: Geo: Japan | ASN: AS62713 | Bytes: ↑10.9 KB ↓31.9 KB

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

Observation: Connessione TCP/ssl. verso simage2.pubmatic.com (103.231.98.194:443). con 11165 bytes inviati e 32674 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

simage2.pubmatic.com (103.231.98.194:443) LOW (33% conf)

Enrichment: Geo: Japan | ASN: AS62713 | Bytes: ↑10.9 KB ↓31.9 KB

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

Observation: Connessione TCP/tls. verso simage2.pubmatic.com (103.231.98.194:443). con 11165 bytes inviati e 32674 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

simage4.pubmatic.com (67.199.150.85:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS62713 | Bytes: ↑3.1 KB ↓9.3 KB

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

Observation: Connessione TCP/ssl. verso simage4.pubmatic.com (67.199.150.85:443). con 3163 bytes inviati e 9498 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

stags.bluekai.com (104.122.80.180:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS8529 | Bytes: ↑2.6 KB ↓11.1 KB

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

Observation: Connessione TCP/ssl. verso stags.bluekai.com (104.122.80.180:443). con 2688 bytes inviati e 11332 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

static-exp1.licdn.com (94.142.38.234:443) LOW (33% conf)

Enrichment: Geo: JO | ASN: AS48832 | Bytes: ↑1.8 KB ↓38.7 KB

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

Observation: Connessione TCP/ssl. verso static-exp1.licdn.com (94.142.38.234:443). con 1825 bytes inviati e 39668 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

static-exp1.licdn.com (94.142.38.210:443) MEDIUM (33% conf)

Enrichment: Geo: JO | ASN: AS48832 | Bytes: ↑14.3 KB ↓420.0 KB

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

Observation: Connessione TCP/ssl. verso static-exp1.licdn.com (94.142.38.210:443). con 14610 bytes inviati e 430029 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

static.criteo.net (178.250.2.130:443) LOW (33% conf)

Enrichment: Geo: France | ASN: ASNA | Bytes: ↑5.2 KB ↓44.3 KB

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

Observation: Connessione TCP/ssl. verso static.criteo.net (178.250.2.130:443). con 5299 bytes inviati e 45391 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

static.criteo.net (178.250.2.130:443) LOW (33% conf)

Enrichment: Geo: France | ASN: ASNA | Bytes: ↑5.2 KB ↓44.3 KB

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

Observation: Connessione TCP/tls. verso static.criteo.net (178.250.2.130:443). con 5299 bytes inviati e 45391 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

stats.g.doubleclick.net (108.177.15.157:443)

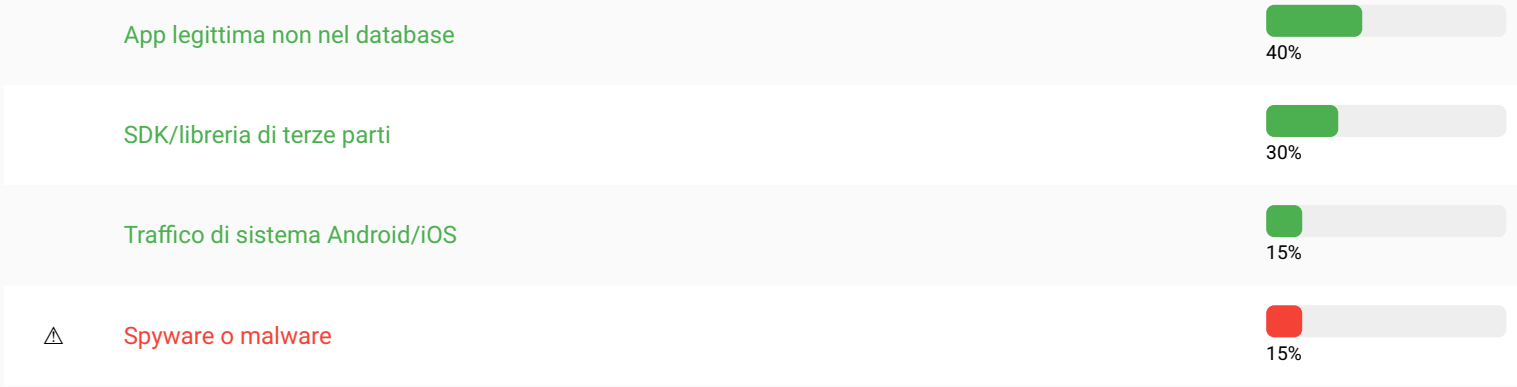
LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑3.2 KB ↓7.8 KB

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

Observation: Connessione TCP/ssl. verso stats.g.doubleclick.net (108.177.15.157:443). con 3253 bytes inviati e 7944 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

sync-tm.everesttech.net (199.232.82.49:443)

LOW (33% conf)

Enrichment: Geo: United States | ASN: AS54113 | Bytes: ↑2.2 KB ↓10.7 KB

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

Observation: Connessione TCP/ssl. verso sync-tm.everesttech.net (199.232.82.49:443). con 2261 bytes inviati e 10948 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

sync.1rx.io (74.118.186.45:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS6336 | Bytes: ↑7.5 KB ↓22.2 KB

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

Observation: Connessione TCP/ssl. verso sync.1rx.io (74.118.186.45:443). con 7677 bytes inviati e 22766 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

sync.crwdcntrl.net (52.76.4.134:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑1.9 KB ↓11.9 KB

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

Observation: Connessione TCP/ssl. verso sync.crwdcntrl.net (52.76.4.134:443). con 1944 bytes inviati e 12154 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

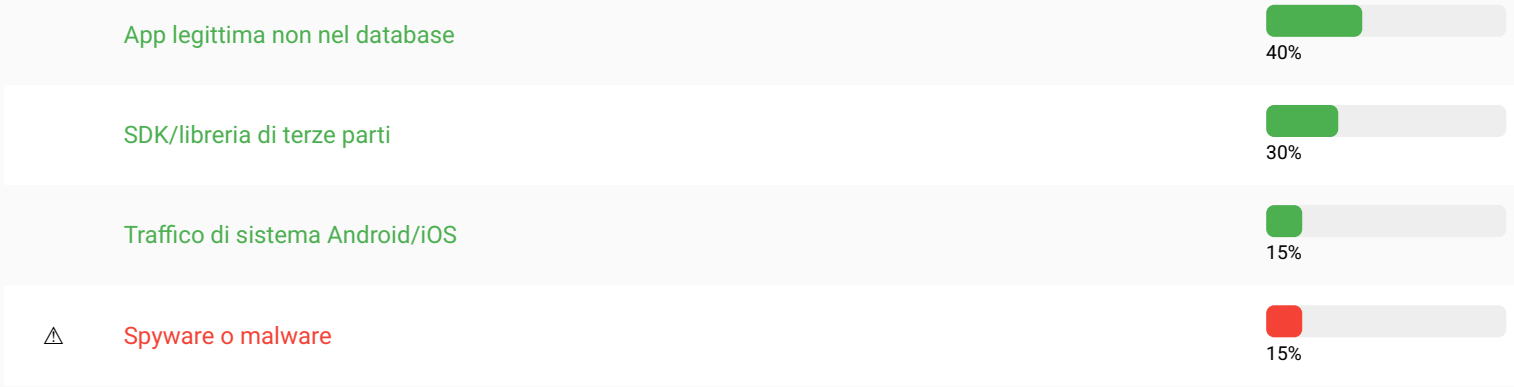
sync.inmobi.com (20.72.149.136:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS8075 | Bytes: ↑1.9 KB ↓15.1 KB

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

Observation: Connessione TCP/ssl. verso sync.inmobi.com (20.72.149.136:443). con 1937 bytes inviati e 15454 bytes ricevuti. [App not identified with significant data transfer].

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

sync.mathtag.com (185.29.132.245:443) LOW (33% conf)

Enrichment: Geo: Belgium | ASN: AS47346 | Bytes: ↑7.1 KB ↓14.0 KB

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

Observation: Connessione TCP/ssl. verso sync.mathtag.com (185.29.132.245:443). con 7321 bytes inviati e 14322 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

tags.rd.linksynergy.com (34.98.67.3:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS396982 | Bytes: ↑1.6 KB ↓9.4 KB

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

Observation: Connessione TCP/ssl. verso tags.rd.linksynergy.com (34.98.67.3:443). con 1686 bytes inviati e 9625 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

tpc.googlesyndication.com (216.58.212.97:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑5.1 KB ↓85.1 KB

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

Observation: Connessione TCP/ssl. verso tpc.googlesyndication.com (216.58.212.97:443). con 5222 bytes inviati e 87115 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

tpc.googlesyndication.com (142.250.185.97:443)

LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑1.4 KB ↓24.2 KB

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

Observation: Connessione TCP/ssl. verso tpc.googlesyndication.com (142.250.185.97:443). con 1484 bytes inviati e 24820 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

trc.taboola.com (151.101.193.44:443)

LOW (33% conf)

Enrichment: Geo: United States | ASN: AS54113 | Bytes: ↑2.1 KB ↓9.1 KB

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

Observation: Connessione TCP/ssl. verso trc.taboola.com (151.101.193.44:443). con 2155 bytes inviati e 9362 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

um.simpli.fi (169.50.137.184:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS36351 | Bytes: ↑2.9 KB ↓13.7 KB

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

Observation: Connessione TCP/ssl. verso um.simpli.fi (169.50.137.184:443). con 2928 bytes inviati e 13983 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

ups.analytics.yahoo.com (18.156.0.31:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑2.9 KB ↓14.7 KB

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

Observation: Connessione TCP/ssl. verso ups.analytics.yahoo.com (18.156.0.31:443). con 2956 bytes inviati e 15052 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

vjs.zencdn.net (151.101.142.217:443)

LOW (33% conf)

Enrichment: Geo: United States | ASN: AS54113 | Bytes: ↑1.6 KB ↓17.3 KB

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

Observation: Connessione TCP/ssl. verso vjs.zencdn.net (151.101.142.217:443). con 1654 bytes inviati e 17737 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

www.aljazeera.net (23.79.129.52:443)

MEDIUM (33% conf)

Enrichment: Geo: United States | ASN: AS20940 | Bytes: ↑30.3 KB ↓1.4 MB

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

Observation: Connessione TCP/ssl. verso www.aljazeera.net (23.79.129.52:443). con 31052 bytes inviati e 1425400 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

www.googletagmanager.com (142.251.37.40:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑1.7 KB ↓81.0 KB

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

Observation: Connessione TCP/ssl. verso www.googletagmanager.com (142.251.37.40:443). con 1728 bytes inviati e 82913 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

www.linkedin.com (13.107.42.14:443) LOW (33% conf)

Enrichment: Geo: United States | ASN: AS8068 | Bytes: ↑25.7 KB ↓40.1 KB

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

Observation: Connessione TCP/ssl. verso www.linkedin.com (13.107.42.14:443). con 26355 bytes inviati e 41081 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

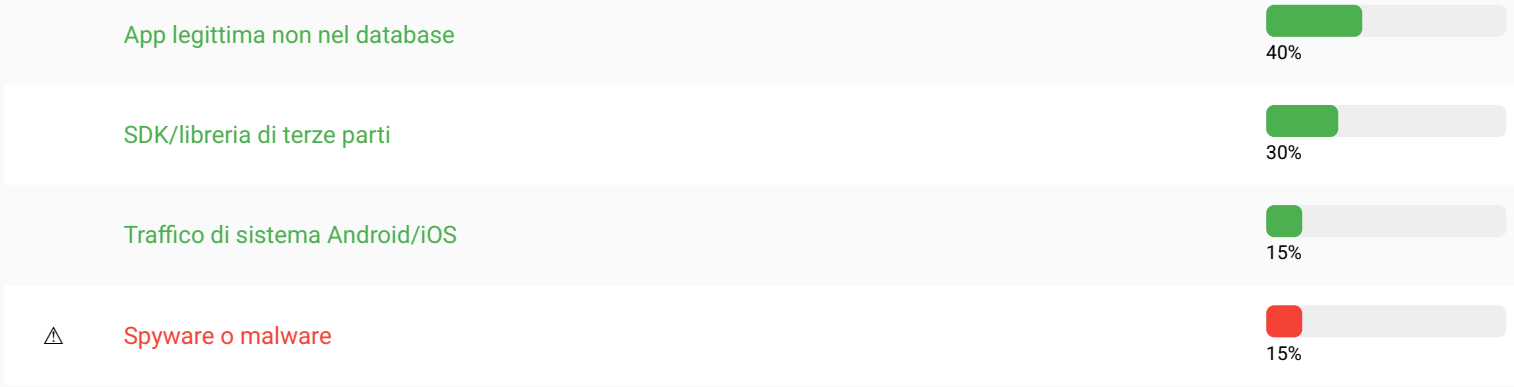
www.youtube.com (172.217.19.46:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS15169 | Bytes: ↑11.8 KB ↓44.0 KB

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

Observation: Connessione TCP/ssl. verso www.youtube.com (172.217.19.46:443). con 12067 bytes inviati e 45064 bytes ricevuti.

Alternative Hypotheses:



Conclusion: Comportamento probabilmente legittimo: App legittima non nel database

x.bidswitch.net (3.121.19.101:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑12.2 KB ↓14.5 KB

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

Observation: Connessione TCP/ssl. verso x.bidswitch.net (3.121.19.101:443). con 12475 bytes inviati e 14818 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

x.bidswitch.net (18.185.222.19:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑2.4 KB ↓10.6 KB

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

Observation: Connessione TCP/tls. verso x.bidswitch.net (18.185.222.19:443). con 2429 bytes inviati e 10838 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

x.bidswitch.net (18.185.222.19:443) LOW (50% conf)

Enrichment: Geo: United States | ASN: AS16509 | Bytes: ↑2.4 KB ↓10.6 KB

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

Observation: Connessione TCP/ssl. verso x.bidswitch.net (18.185.222.19:443). con 2429 bytes inviati e 10838 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

Uncategorized Communications

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	djp.bz	119.8.35.235	443	↑1.1KB ↓274B	--
TCP	http	mpnijffhvaxs	92.242.129.221	80	↑660B ↓160B	--
UDP	dns	--	10.215.173.2	53	↑10.3KB ↓26.3KB	--
TCP	dns	--	10.215.173.2	53	↑10.3KB ↓26.3KB	--
TCP	ssl	--	142.250.200.226	443	↑2.3KB ↓1.4KB	--
UDP	dns	--	8.8.8.8	53	↑717B ↓848B	--
TCP	dns	--	8.8.8.8	53	↑717B ↓848B	--
TCP	ssl	a.pub.network	104.26.0.139	443	↑1.3KB ↓353.1KB	--
TCP	ssl	a.tribalfusion.com	104.18.13.5	443	↑4.4KB ↓8.6KB	--
TCP	tls	a.tribalfusion.com	104.18.13.5	443	↑4.4KB ↓8.6KB	--
TCP	ssl	accounts.google.com	172.217.19.141	443	↑2.0KB ↓3.5KB	--
TCP	ssl	ad-delivery.net	104.26.2.70	443	↑1.6KB ↓6.1KB	--
TCP	ssl	ad.doubleclick.net	142.251.37.198	443	↑1.7KB ↓10.8KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	ad.turn.com	46.228.164.11	443	↑2.4KB ↓15.2KB	--
TCP	ssl	ads.creative-serving.com	3.120.18.167	443	↑4.3KB ↓20.5KB	--
TCP	ssl	ads.playground.xyz	34.102.253.54	443	↑1.7KB ↓11.1KB	--
TCP	ssl	ads.yieldmo.com	54.254.235.164	443	↑6.5KB ↓17.4KB	--
TCP	ssl	ads.yieldmo.com	3.1.139.153	443	↑3.0KB ↓11.4KB	--
TCP	ssl	adservice.google.com	172.217.18.226	443	↑3.3KB ↓10.8KB	--
TCP	ssl	adservice.google.com	142.250.181.226	443	↑1.6KB ↓3.1KB	--
TCP	ssl	adservice.google.jo	172.217.171.194	443	↑4.4KB ↓15.3KB	--
TCP	tls	adservice.google.jo	172.217.171.194	443	↑4.4KB ↓15.3KB	--
TCP	ssl	android.googleapis.com	172.217.171.202	443	↑1.8KB ↓2.0KB	--
TCP	ssl	ap.lijit.com	72.251.249.14	443	↑10.7KB ↓21.5KB	--
TCP	ssl	ap.lijit.com	72.251.249.13	443	↑4.8KB ↓18.3KB	--
TCP	ssl	ap.lijit.com	209.191.163.210	443	↑5.6KB ↓14.0KB	--
TCP	ssl	api.ad.intl.xiaomi.com	47.241.122.70	443	↑990B ↓3.6KB	--
TCP	ssl	api.btloader.com	130.211.23.194	443	↑1.1KB ↓5.3KB	--
TCP	ssl	api.rlcdn.com	34.120.155.137	443	↑1.0KB ↓6.9KB	--
TCP	ssl	app-measurement.com	142.250.185.110	443	↑2.2KB ↓1.1KB	--
TCP	xmpp	app.chat.global.xiaomi.net	161.117.185.166	5222	↑1.1KB ↓171B	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	xmpp	app.chat.global.xiaomi.net	47.241.35.73	5222	↑1.1KB ↓171B	--
TCP	xmpp	app.chat.global.xiaomi.net	47.241.72.88	5222	↑1.1KB ↓183B	--
TCP	ssl	b1sync.zemanta.com	50.31.142.63	443	↑3.6KB ↓10.6KB	--
TCP	ssl	bam.nr-data.net	162.247.242.21	443	↑33.0KB ↓11.1KB	--
UDP	tls	beacons.gcp.gvt2.com	172.217.18.227	443	↑8.1KB ↓3.4KB	--
TCP	ssl	bidder.criteo.com	178.250.2.131	443	↑11.4KB ↓23.7KB	--
TCP	tls	bidder.criteo.com	178.250.2.131	443	↑11.4KB ↓23.7KB	--
TCP	ssl	btloader.com	172.67.70.134	443	↑990B ↓33.4KB	--
TCP	ssl	btlr.sharethrough.com	54.255.100.22	443	↑5.0KB ↓28.8KB	--
TCP	tls	btlr.sharethrough.com	54.255.100.22	443	↑5.0KB ↓28.8KB	--
TCP	tls	btlr.sharethrough.com	54.251.155.125	443	↑4.2KB ↓17.7KB	--
TCP	ssl	btlr.sharethrough.com	54.251.155.125	443	↑4.2KB ↓17.7KB	--
TCP	tls	btlr.sharethrough.com	52.220.250.98	443	↑1.6KB ↓10.5KB	--
TCP	ssl	btlr.sharethrough.com	52.220.250.98	443	↑1.6KB ↓10.5KB	--
TCP	ssl	c.amazon-adsystem.com	52.222.142.111	443	↑7.0KB ↓71.9KB	--
TCP	ssl	c.amazon-adsystem.com	99.86.116.84	443	↑3.9KB ↓7.9KB	--
TCP	ssl	c.deployads.com	52.205.117.34	443		--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
					↑10.4KB ↓30.8KB	
TCP	ssl	c.deployads.com	54.220.62.216	443	↑6.1KB ↓18.0KB	--
TCP	tls	casale-match.dotomi.com	89.207.16.140	443	↑3.0KB ↓12.0KB	--
TCP	ssl	casale-match.dotomi.com	89.207.16.140	443	↑3.0KB ↓12.0KB	--
TCP	ssl	cdn.cookielaw.org	104.16.148.64	443	↑3.7KB ↓164.2KB	--
TCP	tls	cdn.cookielaw.org	104.16.148.64	443	↑3.7KB ↓164.2KB	--
TCP	ssl	cdn.id5-sync.com	46.105.202.126	443	↑1.6KB ↓20.1KB	--
TCP	ssl	connectivitycheck.gstatic.com	142.251.37.163	443	↑1.1KB ↓1.3KB	--
TCP	ssl	connectivitycheck.gstatic.com	142.250.201.3	443	↑1.9KB ↓2.1KB	--
TCP	ssl	core.iprom.net	195.5.165.20	443	↑1.9KB ↓9.6KB	--
TCP	tls	cs.media.net	104.122.80.29	443	↑2.2KB ↓10.0KB	--
TCP	ssl	cs.media.net	104.122.80.29	443	↑2.2KB ↓10.0KB	--
TCP	ssl	csync.loopme.me	23.88.75.187	443	↑1.8KB ↓9.5KB	--
TCP	ssl	d.pub.network	35.201.71.192	443	↑39.0KB ↓47.3KB	--
TCP	ssl	data.adsrvr.org	15.197.193.217	443	↑4.4KB ↓20.6KB	--
TCP	ssl	dialercallinfolookup-pa.googleapis.com	172.217.18.234	443	↑25.6KB ↓135.9KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
UDP	tls	dialercallinfolookup-pa.googleapis.com	172.217.18.234	443	↑25.6KB ↓135.9KB	--
TCP	ssl	dis.criteo.com	178.250.0.163	443	↑1.8KB ↓7.3KB	--
TCP	ssl	dmp.brand-display.com	34.111.151.213	443	↑1.1KB ↓4.4KB	--
TCP	ssl	dps.jp.cinarra.com	18.179.236.28	443	↑1.9KB ↓12.3KB	--
TCP	ssl	dsportal.aljazeera.net	104.18.26.213	443	↑8.4KB ↓6.8KB	--
TCP	ssl	eb2.3lift.com	13.248.245.213	443	↑4.2KB ↓20.1KB	--
TCP	tls	encrypted-tbn0.gstatic.com	216.58.198.78	443	↑4.6KB ↓70.8KB	--
TCP	ssl	encrypted-tbn0.gstatic.com	216.58.198.78	443	↑4.6KB ↓70.8KB	--
TCP	ssl	eus.rubiconproject.com	104.117.200.100	443	↑2.4KB ↓15.3KB	--
TCP	ssl	fastlane.rubiconproject.com	213.19.162.31	443	↑8.9KB ↓21.6KB	--
TCP	ssl	fonts.gstatic.com	142.250.200.195	443	↑1.8KB ↓33.6KB	--
TCP	ssl	freestar-d.openx.net	35.244.159.8	443	↑7.5KB ↓22.7KB	--
TCP	ssl	freestar-io.videoplayerhub.com	172.67.74.207	443	↑1.6KB ↓5.7KB	--
TCP	tls	g.whatsapp.net	157.240.195.54	443	↑2.7KB ↓2.8KB	--
TCP	xmpp	g.whatsapp.net	157.240.195.54	5222	↑2.0KB ↓1.7KB	--
TCP	ssl	geolocation.onetrust.com	104.20.184.68	443	↑1.6KB ↓5.7KB	--
TCP	ssl	gocm.c.appier.net	139.162.38.30	443	↑1.6KB ↓10.6KB	--
TCP	http	google.com	172.217.171.238	80	↑533B ↓616B	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	http	google.com	172.217.171.238	80	↑533B ↓616B	--
TCP	ssl	googleads.g.doubleclick.net	172.217.18.34	443	↑18.8KB ↓77.2KB	--
TCP	tls	googleads.g.doubleclick.net	172.217.18.34	443	↑18.8KB ↓77.2KB	--
TCP	ssl	googleads.g.doubleclick.net	142.250.201.34	443	↑6.5KB ↓29.3KB	--
TCP	ssl	googleads.g.doubleclick.net	142.251.37.162	443	↑3.4KB ↓14.7KB	--
TCP	ssl	gu.dyntrk.com	51.81.106.33	443	↑2.1KB ↓11.4KB	--
TCP	ssl	gum.criteo.com	178.250.0.157	443	↑4.3KB ↓17.5KB	--
TCP	ssl	i.ytimg.com	142.251.37.214	443	↑4.6KB ↓12.0KB	--
UDP	tls	i.ytimg.com	142.251.37.214	443	↑4.6KB ↓12.0KB	--
TCP	ssl	i.ytimg.com	216.58.205.214	443	↑2.4KB ↓22.1KB	--
TCP	ssl	id.crwdcntrl.net	18.139.37.129	443	↑1.1KB ↓6.7KB	--
TCP	ssl	id.google.com	142.251.117.94	443	↑2.2KB ↓15.3KB	--
TCP	ssl	id.rlcdn.com	35.190.60.146	443	↑3.0KB ↓21.2KB	--
TCP	ssl	id.sharedid.org	52.10.19.115	443	↑1.7KB ↓11.6KB	--
TCP	ssl	ipac.ctnsnet.com	35.186.193.173	443	↑1.8KB ↓8.2KB	--
TCP	ssl	js-agent.newrelic.com	199.232.82.137	443	↑989B ↓19.3KB	--
TCP	tls	lh5.googleusercontent.com	172.217.18.225	443	↑2.6KB ↓52.7KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	lh5.googleusercontent.com	172.217.18.225	443	↑2.6KB ↓52.7KB	--
TCP	ssl	live-hls-web-aja.getaj.net	176.29.114.155	443	↑19.5KB ↓9.25MB	--
TCP	tls	live-hls-web-aja.getaj.net	176.29.114.155	443	↑19.5KB ↓9.25MB	--
TCP	ssl	loadm.exelator.com	52.26.6.186	443	↑2.0KB ↓7.5KB	--
TCP	ssl	mab.chartbeat.com	151.101.2.202	443	↑1.1KB ↓5.5KB	--
TCP	ssl	match.deepintent.com	169.197.150.8	443	↑1.7KB ↓7.3KB	--
TCP	ssl	match.sharethrough.com	52.77.1.3	443	↑3.0KB ↓14.1KB	--
TCP	tls	match.sharethrough.com	35.156.177.8	443	↑3.3KB ↓5.9KB	--
TCP	ssl	match.sharethrough.com	35.156.177.8	443	↑3.3KB ↓5.9KB	--
TCP	ssl	metrics.brightcove.com	35.244.232.184	443	↑23.1KB ↓21.4KB	--
TCP	tls	metrics.brightcove.com	35.244.232.184	443	↑23.1KB ↓21.4KB	--
TCP	ssl	mtalk.google.com	173.194.76.188	5228	↑959B ↓850B	--
TCP	ssl	mtalk.google.com	108.177.15.188	5228	↑988B ↓876B	--
TCP	ssl	mtalk.google.com	74.125.206.188	5228	↑4.7KB ↓4.1KB	--
TCP	ssl	mtalk.google.com	64.233.184.188	5228	↑3.0KB ↓2.6KB	--
TCP	tcp	mtalk.google.com	64.233.184.188	5228	↑3.0KB ↓2.6KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	nexus.ensighten.com	52.209.177.22	443	↑2.2KB ↓32.1KB	--
TCP	ssl	p.adsymptotic.com	104.18.98.194	443	↑2.8KB ↓7.6KB	--
TCP	ssl	p.rfihub.com	198.8.71.128	443	↑2.1KB ↓7.3KB	--
TCP	ssl	pagead2.googleadservices.com	142.250.200.194	443	↑9.1KB ↓5.0KB	--
TCP	ssl	pagead2.googlesyndication.com	142.251.37.194	443	↑7.5KB ↓9.0KB	--
TCP	ssl	pagead2.googlesyndication.com	142.250.203.226	443	↑7.6KB ↓78.4KB	--
TCP	ssl	pagead2.googlesyndication.com	172.217.21.2	443	↑10.7KB ↓25.3KB	--
UDP	tls	pagead2.googlesyndication.com	142.251.37.194	443	↑7.5KB ↓9.0KB	--
TCP	tls	pagead2.googlesyndication.com	172.217.21.2	443	↑10.7KB ↓25.3KB	--
TCP	ssl	pghub.io	35.241.45.217	443	↑1.6KB ↓12.1KB	--
TCP	ssl	ping.chartbeat.net	23.20.220.210	443	↑4.6KB ↓8.4KB	--
TCP	ssl	ping.chartbeat.net	3.211.176.233	443	↑2.3KB ↓7.4KB	--
TCP	ssl	pippio.com	107.178.254.65	443	↑2.0KB ↓11.2KB	--
TCP	ssl	pixel-eu.rubiconproject.com	69.173.144.138	443	↑2.1KB ↓6.7KB	--
TCP	ssl	pixel-eu.rubiconproject.com	69.173.144.165	443	↑4.6KB ↓10.9KB	--
TCP	ssl	pixel-eu.rubiconproject.com	69.173.144.139	443	↑6.4KB ↓14.7KB	--
TCP	ssl	pixel-sync.sitescout.com	66.155.71.150	443	↑2.0KB ↓9.0KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	tls	pixel-sync.sitescout.com	66.155.71.25	443	↑2.7KB ↓7.2KB	--
TCP	ssl	pixel-sync.sitescout.com	66.155.71.25	443	↑2.7KB ↓7.2KB	--
TCP	ssl	pixel.tapad.com	35.227.248.159	443	↑1.6KB ↓5.0KB	--
UDP	tls	play-lh.googleusercontent.com	142.250.203.246	443	↑4.6KB ↓12.1KB	--
TCP	ssl	players.brightcove.net	104.122.81.100	443	↑1.0KB ↓243.6KB	--
TCP	ssl	pm.w55c.net	13.228.74.15	443	↑4.6KB ↓18.8KB	--
TCP	ssl	pool.admedo.com	35.210.53.219	443	↑2.7KB ↓13.5KB	--
TCP	tls	pr-bh.ybp.yahoo.com	54.75.169.44	443	↑2.2KB ↓12.4KB	--
TCP	ssl	pr-bh.ybp.yahoo.com	54.75.169.44	443	↑2.2KB ↓12.4KB	--
TCP	ssl	pro.ip-api.com	208.95.112.2	443	↑2.4KB ↓6.0KB	--
TCP	ssl	push.mobilefonex.com	119.8.47.97	443	↑6.3KB ↓32.9KB	--
TCP	ssl	resolver.msg.global.xiaomi.net	47.241.56.51	443	↑1.1KB ↓3.9KB	--
TCP	ssl	rtb.gumgum.com	54.178.144.187	443	↑1.8KB ↓11.4KB	--
TCP	ssl	rtb.openx.net	35.227.252.103	443	↑1.9KB ↓8.3KB	--
TCP	ssl	rules.quantcount.com	52.222.137.87	443	↑2.1KB ↓16.7KB	--
TCP	ssl	sb.scorecardresearch.com	52.222.137.28	443	↑2.5KB ↓9.2KB	--
TCP	ssl	secure.cdn.fastclick.net	23.222.56.60	443	↑1.6KB ↓25.3KB	--
TCP	ssl	secure.quantserve.com	91.228.74.202	443	↑2.7KB ↓18.2KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	secure.quantserve.com	91.228.74.133	443	↑2.0KB ↓6.0KB	--
TCP	tls	secure.quantserve.com	91.228.74.133	443	↑2.0KB ↓6.0KB	--
TCP	ssl	securepubads.g.doubleclick.net	172.217.171.226	443	↑31.0KB ↓240.4KB	--
TCP	tls	securepubads.g.doubleclick.net	172.217.171.226	443	↑31.0KB ↓240.4KB	--
TCP	ssl	ssl.gstatic.com	142.251.37.227	443	↑584B ↓5.7KB	--
TCP	ssl	ssl.gstatic.com	172.217.171.227	443	↑8.5KB ↓77.5KB	--
TCP	ssl	stags.bluekai.com	104.122.80.180	443	↑2.6KB ↓11.1KB	--
TCP	ssl	static-exp1.licdn.com	94.142.38.234	443	↑1.8KB ↓38.7KB	--
TCP	ssl	static-exp1.licdn.com	94.142.38.210	443	↑14.3KB ↓420.0KB	--
TCP	ssl	static.chartbeat.com	13.227.217.7	443	↑2.1KB ↓34.1KB	--
TCP	ssl	static.criteo.net	178.250.2.130	443	↑5.2KB ↓44.3KB	--
TCP	tls	static.criteo.net	178.250.2.130	443	↑5.2KB ↓44.3KB	--
TCP	ssl	stats.g.doubleclick.net	108.177.15.157	443	↑3.2KB ↓7.8KB	--
TCP	ssl	sync-dsp.ad-m.asia	202.131.200.84	443	↑2.0KB ↓7.1KB	--
TCP	ssl	sync.1rx.io	74.118.186.45	443	↑7.5KB ↓22.2KB	--
TCP	ssl	sync.crwdcntrl.net	52.76.4.134	443	↑1.9KB ↓11.9KB	--
TCP	ssl	sync.mathtag.com	185.29.132.245	443	↑7.1KB ↓14.0KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	tags.rd.linksynergy.com	34.98.67.3	443	↑1.6KB ↓9.4KB	--
TCP	ssl	tlx.3lift.com	54.93.106.38	443	↑4.6KB ↓17.1KB	--
TCP	ssl	tlx.3lift.com	3.124.152.204	443	↑2.8KB ↓11.9KB	--
TCP	ssl	tpc.googlesyndication.com	216.58.212.97	443	↑5.1KB ↓85.1KB	--
TCP	ssl	tpc.googlesyndication.com	142.250.185.97	443	↑1.4KB ↓24.2KB	--
TCP	ssl	trc.taboola.com	151.101.193.44	443	↑2.1KB ↓9.1KB	--
TCP	ssl	uipglob.semasio.net	77.243.60.138	443	↑2.3KB ↓7.5KB	--
TCP	ssl	ups.analytics.yahoo.com	18.156.0.31	443	↑2.9KB ↓14.7KB	--
TCP	ssl	www.aljazeera.net	23.79.129.52	443	↑30.3KB ↓1.36MB	--
UDP	tls	www.google.com	142.251.37.36	443	↑23.2KB ↓9.5KB	--
TCP	ssl	www.google.com	142.251.37.36	443	↑23.2KB ↓9.5KB	--
TCP	ssl	www.google.com	172.217.21.4	443	↑34.6KB ↓1.32MB	--
TCP	ssl	www.google.com	142.250.186.132	443	↑2.5KB ↓2.0KB	--
UDP	quic,ssl	www.googleapis.com	142.250.200.202	443	↑20.0KB ↓10.8KB	--
TCP	ssl	www.googleapis.com	142.251.37.202	443	↑10.8KB ↓3.6KB	--
TCP	ssl	www.googleapis.com	172.217.171.234	443	↑3.9KB ↓13.3KB	--
TCP	ssl	www.googleapis.com	142.251.37.42	443	↑8.4KB ↓20.3KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	www.googleapis.com	142.250.200.234	443	↑656B ↓820B	--
TCP	ssl	www.googleapis.com	142.250.200.202	443	↑20.0KB ↓10.8KB	--
TCP	ssl	www.googleapis.com	216.58.198.74	443	↑1.8KB ↓3.7KB	--
UDP	quic,ssl	www.googleapis.com	142.251.37.42	443	↑8.4KB ↓20.3KB	--
TCP	ssl	www.googletagmanager.com	142.251.37.40	443	↑1.7KB ↓81.0KB	--
TCP	tls	www.gstatic.com	216.58.198.67	443	↑4.8KB ↓90.2KB	--
TCP	ssl	www.gstatic.com	216.58.198.67	443	↑4.8KB ↓90.2KB	--
UDP	tls	www.youtube.com	216.58.211.206	443	↑7.7KB ↓36.0KB	--
UDP	tls	www.youtube.com	172.217.18.46	443	↑3.9KB ↓6.8KB	--
TCP	ssl	www.youtube.com	142.250.201.46	443	↑6.3KB ↓18.0KB	--
TCP	ssl	www.youtube.com	172.217.19.46	443	↑11.8KB ↓44.0KB	--
UDP	tls	www.youtube.com	142.250.201.46	443	↑6.3KB ↓18.0KB	--
TCP	ssl	www.youtube.com	142.250.201.14	443	↑1.9KB ↓47.1KB	--
TCP	ssl	www.youtube.com	142.251.37.206	443	↑3.5KB ↓16.6KB	--
TCP	ssl	www.youtube.com	172.217.21.14	443	↑1.6KB ↓8.2KB	--
TCP	ssl	x.bidswitch.net	3.121.19.101	443	↑12.2KB ↓14.5KB	--
TCP	tls	x.bidswitch.net	18.185.222.19	443	↑2.4KB ↓10.6KB	--

Protocol	App protocol	Domain	Dst IP address	Dst port number	Bytes (↑up ↓down)	Flow Diagram
TCP	ssl	x.bidswitch.net	18.185.222.19	443	↑2.4KB ↓10.6KB	--

Whitelisted communications

Protocol	Domain	Dst IP address	Dst port number
UDP	--	10.215.173.2	53
TCP	--	10.215.173.2	53
TCP	--	142.250.200.226	443
TCP	62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com	199.127.194.97	443
TCP	62ea30a39dede4f6d44ac289591051076c294526.cws.conviva.com	199.127.193.108	443
UDP	--	8.8.8.8	53
TCP	--	8.8.8.8	53
TCP	a.pub.network	104.26.0.139	443
TCP	a.tribalfusion.com	104.18.13.5	443
TCP	a.tribalfusion.com	104.18.13.5	443
TCP	aax-eu.amazon-adsystem.com	54.239.38.253	443
TCP	accounts.google.com	172.217.19.141	443
TCP	acdn.adnxs.com	151.101.141.108	443

Protocol	Domain	Dst IP address	Dst port number
TCP	ad-delivery.net	104.26.2.70	443
TCP	ad.doubleclick.net	142.251.37.198	443
TCP	ad.turn.com	46.228.164.11	443
TCP	ads.creative-serving.com	3.120.18.167	443
TCP	ads.playground.xyz	34.102.253.54	443
TCP	ads.pubmatic.com	104.122.80.250	443
TCP	ads.yieldmo.com	54.254.235.164	443
TCP	ads.yieldmo.com	3.1.139.153	443
TCP	adservice.google.com	172.217.18.226	443
TCP	adservice.google.com	142.250.181.226	443
TCP	adservice.google.jo	172.217.171.194	443
TCP	adservice.google.jo	172.217.171.194	443
TCP	ae.linkedin.com	144.2.15.5	443
TCP	android.googleapis.com	172.217.171.202	443
TCP	ap.lijit.com	72.251.249.14	443
TCP	ap.lijit.com	72.251.249.13	443
TCP	ap.lijit.com	209.191.163.210	443
TCP	api.ad.intl.xiaomi.com	47.241.122.70	443

Protocol	Domain	Dst IP address	Dst port number
TCP	api.btloader.com	130.211.23.194	443
TCP	api.rlcdn.com	34.120.155.137	443
TCP	app-measurement.com	142.250.185.110	443
TCP	app.chat.global.xiaomi.net	161.117.185.166	5222
TCP	app.chat.global.xiaomi.net	47.241.35.73	5222
TCP	app.chat.global.xiaomi.net	47.241.72.88	5222
TCP	b1sync.zemanta.com	50.31.142.63	443
TCP	bam.nr-data.net	162.247.242.21	443
UDP	beacons.gcp.gvt2.com	172.217.18.227	443
TCP	bidder.criteo.com	178.250.2.131	443
TCP	bidder.criteo.com	178.250.2.131	443
TCP	btloader.com	172.67.70.134	443
TCP	btlr.sharethrough.com	54.255.100.22	443
TCP	btlr.sharethrough.com	54.255.100.22	443
TCP	btlr.sharethrough.com	54.251.155.125	443
TCP	btlr.sharethrough.com	54.251.155.125	443
TCP	btlr.sharethrough.com	52.220.250.98	443
TCP	btlr.sharethrough.com	52.220.250.98	443

Protocol	Domain	Dst IP address	Dst port number
TCP	bttrack.com	192.132.33.46	443
TCP	c.amazon-adsystem.com	52.222.142.111	443
TCP	c.amazon-adsystem.com	99.86.116.84	443
TCP	c.bing.com	204.79.197.200	443
TCP	c.deployads.com	52.205.117.34	443
TCP	c.deployads.com	54.220.62.216	443
TCP	c1.adform.net	185.84.60.20	443
TCP	c1.adform.net	185.84.60.20	443
TCP	casale-match.dotomi.com	89.207.16.140	443
TCP	casale-match.dotomi.com	89.207.16.140	443
TCP	cdn.ampproject.org	142.250.200.193	443
TCP	cdn.cookielaw.org	104.16.148.64	443
TCP	cdn.cookielaw.org	104.16.148.64	443
TCP	cdn.id5-sync.com	46.105.202.126	443
TCP	client.mobilefonex.com	159.138.146.100	80
TCP	cm.adgrx.com	63.251.232.170	443
TCP	connectivitycheck.gstatic.com	142.251.37.163	443
TCP	connectivitycheck.gstatic.com	142.250.201.3	443

Protocol	Domain	Dst IP address	Dst port number
TCP	core.iprom.net	195.5.165.20	443
TCP	cs.media.net	104.122.80.29	443
TCP	cs.media.net	104.122.80.29	443
TCP	csync.loopme.me	23.88.75.187	443
TCP	d.pub.network	35.201.71.192	443
TCP	data.adsrvr.org	15.197.193.217	443
TCP	dialercallinfolookup-pa.googleapis.com	172.217.18.234	443
UDP	dialercallinfolookup-pa.googleapis.com	172.217.18.234	443
TCP	dis.criteo.com	178.250.0.163	443
TCP	dmp.brand-display.com	34.111.151.213	443
TCP	dps.jp.cinarra.com	18.179.236.28	443
TCP	dsportal.aljazeera.net	104.18.26.213	443
TCP	eb2.3lift.com	13.248.245.213	443
TCP	edge.api.brightcove.com	151.101.142.27	443
TCP	encrypted-tbn0.gstatic.com	216.58.198.78	443
TCP	encrypted-tbn0.gstatic.com	216.58.198.78	443
TCP	eus.rubiconproject.com	104.117.200.100	443
TCP	fastlane.rubiconproject.com	213.19.162.31	443

Protocol	Domain	Dst IP address	Dst port number
TCP	fonts.gstatic.com	142.250.200.195	443
TCP	freestar-d.openx.net	35.244.159.8	443
TCP	freestar-io.videoplayerhub.com	172.67.74.207	443
TCP	g.whatsapp.net	157.240.195.54	443
TCP	g.whatsapp.net	157.240.195.54	5222
TCP	geolocation.onetrust.com	104.20.184.68	443
TCP	gocm.c.appier.net	139.162.38.30	443
TCP	google.com	172.217.171.238	80
TCP	google.com	172.217.171.238	80
TCP	googleads.g.doubleclick.net	172.217.18.34	443
TCP	googleads.g.doubleclick.net	172.217.18.34	443
TCP	googleads.g.doubleclick.net	142.250.201.34	443
TCP	googleads.g.doubleclick.net	142.251.37.162	443
TCP	gu.dyntrk.com	51.81.106.33	443
TCP	gum.criteo.com	178.250.0.157	443
TCP	hbopenbid.pubmatic.com	103.231.98.193	443
TCP	htlb.casalemedia.com	2.21.111.28	443
TCP	htlb.casalemedia.com	2.21.111.28	443

Protocol	Domain	Dst IP address	Dst port number
TCP	i.ytimg.com	142.251.37.214	443
UDP	i.ytimg.com	142.251.37.214	443
TCP	i.ytimg.com	216.58.205.214	443
TCP	ib.adnxs.com	185.33.220.216	443
TCP	ib.adnxs.com	185.33.221.53	443
TCP	id.crwdcntrl.net	18.139.37.129	443
TCP	id.google.com	142.251.117.94	443
TCP	id.rlcdn.com	35.190.60.146	443
TCP	id.sharedid.org	52.10.19.115	443
TCP	id5-sync.com	51.89.21.5	443
TCP	image4.pubmatic.com	103.231.98.195	443
TCP	image6.pubmatic.com	103.231.98.196	443
TCP	inbox.google.com	172.217.171.197	443
TCP	ipac.ctnsnet.com	35.186.193.173	443
TCP	js-agent.newrelic.com	199.232.82.137	443
TCP	js-sec.indexww.com	104.122.81.53	443
TCP	lh5.googleusercontent.com	172.217.18.225	443
TCP	lh5.googleusercontent.com	172.217.18.225	443

Protocol	Domain	Dst IP address	Dst port number
TCP	live-hls-web-aja.getaj.net	176.29.114.155	443
TCP	live-hls-web-aja.getaj.net	176.29.114.155	443
TCP	loadm.exelator.com	52.26.6.186	443
TCP	mab.chartbeat.com	151.101.2.202	443
TCP	match.deepintent.com	169.197.150.8	443
TCP	match.prod.bidr.io	54.236.195.76	443
TCP	match.sharethrough.com	52.77.1.3	443
TCP	match.sharethrough.com	35.156.177.8	443
TCP	match.sharethrough.com	35.156.177.8	443
TCP	metrics.brightcove.com	35.244.232.184	443
TCP	metrics.brightcove.com	35.244.232.184	443
TCP	mtalk.google.com	173.194.76.188	5228
TCP	mtalk.google.com	108.177.15.188	5228
TCP	mtalk.google.com	74.125.206.188	5228
TCP	mtalk.google.com	64.233.184.188	5228
TCP	mtalk.google.com	64.233.184.188	5228
TCP	nexus.ensighten.com	52.209.177.22	443
TCP	p.adsymptotic.com	104.18.98.194	443

Protocol	Domain	Dst IP address	Dst port number
TCP	p.rfihub.com	198.8.71.128	443
TCP	pagead2.googleadservices.com	142.250.200.194	443
TCP	pagead2.googlesyndication.com	142.251.37.194	443
TCP	pagead2.googlesyndication.com	142.250.203.226	443
TCP	pagead2.googlesyndication.com	172.217.21.2	443
UDP	pagead2.googlesyndication.com	142.251.37.194	443
TCP	pagead2.googlesyndication.com	172.217.21.2	443
TCP	pghub.io	35.241.45.217	443
TCP	ping.chartbeat.net	23.20.220.210	443
TCP	ping.chartbeat.net	3.211.176.233	443
TCP	pippio.com	107.178.254.65	443
TCP	pixel-eu.rubiconproject.com	69.173.144.138	443
TCP	pixel-eu.rubiconproject.com	69.173.144.165	443
TCP	pixel-eu.rubiconproject.com	69.173.144.139	443
TCP	pixel-sync.sitescout.com	66.155.71.150	443
TCP	pixel-sync.sitescout.com	66.155.71.25	443
TCP	pixel-sync.sitescout.com	66.155.71.25	443
TCP	pixel.tapad.com	35.227.248.159	443

Protocol	Domain	Dst IP address	Dst port number
UDP	play-lh.googleusercontent.com	142.250.203.246	443
TCP	players.brightcove.net	104.122.81.100	443
TCP	pm.w55c.net	13.228.74.15	443
TCP	pool.admedo.com	35.210.53.219	443
TCP	pr-bh.ybp.yahoo.com	54.75.169.44	443
TCP	pr-bh.ybp.yahoo.com	54.75.169.44	443
TCP	pro.ip-api.com	208.95.112.2	443
TCP	push.mobilefonex.com	119.8.47.97	443
TCP	resolver.msg.global.xiaomi.net	47.241.56.51	443
TCP	rtb.adentifi.com	54.174.34.153	443
TCP	rtb.gumgum.com	54.178.144.187	443
TCP	rtb.openx.net	35.227.252.103	443
TCP	rules.quantcount.com	52.222.137.87	443
TCP	s.amazon-adsystem.com	209.54.180.3	443
TCP	sb.scorecardresearch.com	52.222.137.28	443
TCP	secure.cdn.fastclick.net	23.222.56.60	443
TCP	secure.quantserve.com	91.228.74.202	443
TCP	secure.quantserve.com	91.228.74.133	443

Protocol	Domain	Dst IP address	Dst port number
TCP	secure.quantserve.com	91.228.74.133	443
TCP	securepubads.g.doubleclick.net	172.217.171.226	443
TCP	securepubads.g.doubleclick.net	172.217.171.226	443
TCP	simage2.pubmatic.com	103.231.98.194	443
TCP	simage2.pubmatic.com	103.231.98.194	443
TCP	simage4.pubmatic.com	67.199.150.85	443
TCP	ssl.gstatic.com	142.251.37.227	443
TCP	ssl.gstatic.com	172.217.171.227	443
TCP	stags.bluekai.com	104.122.80.180	443
TCP	static-exp1.licdn.com	94.142.38.234	443
TCP	static-exp1.licdn.com	94.142.38.210	443
TCP	static.chartbeat.com	13.227.217.7	443
TCP	static.criteo.net	178.250.2.130	443
TCP	static.criteo.net	178.250.2.130	443
TCP	stats.g.doubleclick.net	108.177.15.157	443
TCP	sync-dsp.ad-m.asia	202.131.200.84	443
TCP	sync-tm.everesttech.net	199.232.82.49	443
TCP	sync.1rx.io	74.118.186.45	443

Protocol	Domain	Dst IP address	Dst port number
TCP	sync.crwdcntrl.net	52.76.4.134	443
TCP	sync.inmobi.com	20.72.149.136	443
TCP	sync.mathtag.com	185.29.132.245	443
TCP	sync.technoratimedia.com	193.122.130.38	443
TCP	tags.rd.linksynergy.com	34.98.67.3	443
TCP	tlx.3lift.com	54.93.106.38	443
TCP	tlx.3lift.com	3.124.152.204	443
TCP	tpc.googlesyndication.com	216.58.212.97	443
TCP	tpc.googlesyndication.com	142.250.185.97	443
TCP	trc.taboola.com	151.101.193.44	443
TCP	uipglob.semasio.net	77.243.60.138	443
TCP	um.simpli.fi	169.50.137.184	443
TCP	ups.analytics.yahoo.com	18.156.0.31	443
TCP	vjs.zencdn.net	151.101.142.217	443
TCP	www.aljazeera.net	23.79.129.52	443
UDP	www.google.com	142.251.37.36	443
TCP	www.google.com	142.251.37.36	443
TCP	www.google.com	172.217.21.4	443

Protocol	Domain	Dst IP address	Dst port number
TCP	www.google.com	142.250.186.132	443
UDP	www.googleapis.com	142.250.200.202	443
TCP	www.googleapis.com	142.251.37.202	443
TCP	www.googleapis.com	172.217.171.234	443
TCP	www.googleapis.com	142.251.37.42	443
TCP	www.googleapis.com	142.250.200.234	443
TCP	www.googleapis.com	142.250.200.202	443
TCP	www.googleapis.com	216.58.198.74	443
UDP	www.googleapis.com	142.251.37.42	443
TCP	www.googletagmanager.com	142.251.37.40	443
TCP	www.gstatic.com	216.58.198.67	443
TCP	www.gstatic.com	216.58.198.67	443
TCP	www.linkedin.com	13.107.42.14	443
UDP	www.youtube.com	216.58.211.206	443
UDP	www.youtube.com	172.217.18.46	443
TCP	www.youtube.com	142.250.201.46	443
TCP	www.youtube.com	172.217.19.46	443
UDP	www.youtube.com	142.250.201.46	443

Protocol	Domain	Dst IP address	Dst port number
TCP	www.youtube.com	142.250.201.14	443
TCP	www.youtube.com	142.251.37.206	443
TCP	www.youtube.com	172.217.21.14	443
TCP	x.bidswitch.net	3.121.19.101	443
TCP	x.bidswitch.net	18.185.222.19	443
TCP	x.bidswitch.net	18.185.222.19	443