8	INF	ORM	ATIC	NC

## **Raw Logs**

# **▲ TLS/SSL Security Tester**

TESTS ♣	RESULT .
Cleartext Traffic Test	<b>~</b>
TLS Misconfiguration Test	×
TLS Pinning/Certificate Transparency Bypass Test	×
TLS Pinning/Certificate Transparency Test	×

Showing 1 to 4 of 4 entries

<u>Previous</u>	1	<u>Next</u>
-----------------	---	-------------

# ● EXPORTED ACTIVITY TESTER

Search:

Search:

SCREENSHOT	ACTIVITY	
No data available in tabl	9	

Showing 0 to 0 of 0 entries

<u>Previous</u> <u>Next</u>

Search:

### **△**■ ACTIVITY TESTER

SCREENSHOT	•	ACTIVITY	\$
	No data available in table	e	

Showing 0 to 0 of 0 entries

Previous	Next
<u>Previous</u>	Next

## **SCREENSHOTS**

# **❖** RUNTIME DEPENDENCIES

com.onesignal.core.internal.application com.onesignal.core.internal.device com.adobe.air.gestures com.onesignal.user.internal.backend io.grpc.internal io.grpc.okhttp.internal elkk io.grpc.okhttp.internal.framed com.adobe.air

com.bumptech.glide.load

io.reactivex.internal.subscriptions

io.reactivex.subjects

gov.nist.javax.sip

dsua

io.reactivex

io.reactivex.internal.operators.maybe

efad

com.onesignal.session.internal.influence

org.reactivestreams

com.adobe.fre

com.onesignal.user.internal.subscriptions

io. reactive x. in ternal. operators. flowable

io.reactivex.internal.schedulers

ezir

com.squareup.okhttp

io.reactivex.internal.util

io.grpc.okhttp

com.onesignal.common

com.bumptech.glide

com.onesignal.core.internal.operations

m

io.grpc.stub

ejnr

com.onesignal.debug

io.reactivex.internal.disposables

io.grpc

com.onesignal.common.services

## SERVER LOCATIONS



This app may communicate with the following OFAC sanctioned list of countries.

	Searcn:	
DOMAIN \$	COUNTRY/REGION \$	
No data available in table		

Showing 0 to 0 of 0 entries

<u>Previous</u>	Next

## **Q** DOMAIN MALWARE CHECK

DOMAIN .	STATUS .	GEOLOCATION
api.onesignal.com	good	IP: 104.16.160.145  Country: United States of America  Region: California  City: San Francisco  Latitude: 37.775700  Longitude: -122.395203  View: Google Map
firebaseinappmessaging.googleapis.com	good	IP: 142.251.32.74  Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
hasofferstracking.betterhelp.com	good	IP: 18.205.37.232  Country: United States of America  Region: Virginia  City: Ashburn  Latitude: 39.043720  Longitude: -77.487488  View: Google Map
nomo-4a867.firebaseio.com	good	IP: 34.120.206.254  Country: United States of America  Region: Missouri  City: Kansas City  Latitude: 39.099731  Longitude: -94.578568  View: Google Map

DOMAIN •	STATUS	GEOLOCATION
nomo-app.s3.us-west-2.amazonaws.com	good	IP: 3.5.78.158  Country: United States of America  Region: Oregon  City: Portland  Latitude: 45.523449  Longitude: -122.676208  View: Google Map
play-fe.googleapis.com	good	IP: 142.251.32.78  Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514  View: Google Map
play.googleapis.com	good	IP: 216.239.32.223  Country: United States of America Region: California City: Mountain View Latitude: 37.405991 Longitude: -122.078514 View: Google Map
s3-us-west-2.amazonaws.com	good	IP: 52.92.233.240  Country: United States of America  Region: Oregon  City: Portland  Latitude: 45.523449  Longitude: -122.676208  View: Google Map

DOMAIN \$	STATUS •	GEOLOCATION
saynomo.com	good	IP: 104.238.101.60  Country: United States of America  Region: Arizona  City: Scottsdale  Latitude: 33.601974  Longitude: -111.887917  View: Google Map
source.android.com	good	IP: 142.251.33.174  Country: United States of America  Region: California  City: Mountain View  Latitude: 37.405991  Longitude: -122.078514  View: Google Map

Showing 1 to 10 of 10 entries

Previous 1 Next

## **CLIPBOARD DUMP**

## **URLS**

https://api.one signal.com/apps/60 feb3d7-28e7-4ef4-a12d-48531a9882 f4/subscriptions/d4698 fcf-ec52-45 fc-ac73-6fb95a6234b4/iams

https://firebase in appmess aging. googleap is. com/google. internal. firebase. in appmess aging. v1. sdks erving. in appmess agings dkserving/fetcheligible campaigns. v2. sdks erving. in appmess agings dkserving. in appmess aging sdkserving. v2. sdkserving. v3. sdkserving. v4. sdkse

https://saynomo.com/donate.php

 $https://source.and roid.com/security/selinux/device-policy \#label\_new\_services\_and\_address\_denials$ 

https://nomo-app.s3.us-west-2.amazonaws.com/ads/images/ad\_better\_help.png

file:///data/app/vmdl1420421607.tmp

https://play.googleapis.com/play/log?format=raw&proto\_v2=true

https://s3-us-west-2.amazonaws.com/nomo-app/ads/ad.xml

https://play.googleapis.com/play/log/timestamp

https://api.onesignal.com/apps/60feb3d7-28e7-4ef4-a12d-48531a9882f4/users/by/onesignal\_id/a29177cf-0065-42aa-a7f8-b3bf668c18ef

https://play-fe.googleapis.com/fdfe/apps/contentsync

https://api.onesignal.com/apps/60feb3d7-28e7-4ef4-a12d-48531a9882f4/android\_params.js?player\_id=d4698fcf-ec52-45fc-ac73-6fb95a6234b4

https://nomo-4a867.firebaseio.com

https://play.googleapis.com/play/log

https://api.onesignal.com/apps/60feb3d7-28e7-4ef4-a12d-48531a9882f4/subscriptions/d4698fcf-ec52-45fc-ac73-6fb95a6234b4

https://hasofferstracking.betterhelp.com/aff\_c?offer\_id=2&aff\_id=1213

https://play-fe.googleapis.com/fdfe/apps/contentsync?nocache\_qos=lt

https://nomo-app.s3.us-west-2.amazonaws.com/ads/images/ad5.png

#### **EMAILS**

244534026@24.45
genymotion-build@genymobile.com
maxk@qualcomm.com
tigran@aivazian.fsnet
dm-devel@redhat.com
giometti@linux.it
tsbogend@alpha.franken

### # TRACKERS

Search:

TRACKER NAME	•	CATEGORIES \$	URL	
OneSignal			https://reports.exodus-privacy.eu.org/trackers/193	

Showing 1 to 1 of 1 entries

<u>Previous</u>	1	<u>Next</u>
Previous	T	<u>Next</u>

## **♣** BASE64 STRINGS DECODED

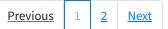
		Search:		
CALLED	<b>♦</b> DECODED STRING			<b>*</b>
	No data available in table			
Showing 0 to 0 of 0 entries				
			<u>Previous</u>	<u>Next</u>
SQLITE DATABASE				
S 26TILE DVIVDV2F				
		Search:		
FILES				*
data/data/air.com.parkerstech.day/datab	bases/com.google.android.datatransport.events			
data/data/air.com.parkerstech.day/datab	bases/google app measurement local.db			
data/data/air.com.parkerstech.day/datab	bases/OneSignal.db			
data/data/air.com.parkerstech.day/no_b	<u>vackup/androidx.work.workdb</u>			
Showing 1 to 4 of 4 entries				
			Previous 1	<u>Next</u>

**XML FILES** 

Search:	
FILES	
data/data/air.com.parkerstech.day/cache/app/6e055251-f268-45fd-b292-4556215d9ff7/assets/META-INF/AIR/application.xml	
data/data/air.com.parkerstech.day/shared_prefs/air.com.parkerstech.day_preferences.xml	
data/data/air.com.parkerstech.day/shared_prefs/com.google.android.gms.appid.xml	
data/data/air.com.parkerstech.day/shared_prefs/com.google.android.gms.measurement.prefs.xml	
data/data/air.com.parkerstech.day/shared_prefs/com.google.firebase.crashlytics.xml	
data/data/air.com.parkerstech.day/shared_prefs/com.google.firebase.inappmessaging.xml	
data/data/air.com.parkerstech.day/shared_prefs/com.google.firebase.messaging.xml	
data/data/air.com.parkerstech.day/shared_prefs/FirebaseHeartBeatT05FU0lHTkFMX1NES19GQ01fQVBQX05BTUU+MTo3NTQ3OTU2MTQwNDl	6YW5kcm9pZDpjNjgyYjgxNDRl
data/data/air.com.parkerstech.day/shared_prefs/FirebaseHeartBeatW0RFRkFVTFRd+MTo4MjMwMzk1MzQ0NDk6YW5kcm9pZDo1NTNhMGE1N	1TdiN2FjOTgy.xml
data/data/air.com.parkerstech.day/shared_prefs/GTPlayerPurchases.xml	
Showing 1 to 10 of 11 entries	
	Previous 1 2 Next
	,
B OTHER FILES	
Search:	

**FILES** data/data/air.com.parkerstech.day/cache/.AIR/certificates/curl-ca-bundle.crt data/data/air.com.parkerstech.day/cache/.AIR/cookies data/data/air.com.parkerstech.day/cache/app/6e055251-f268-45fd-b292-4556215d9ff7/assets/nomo\_android.swf data/data/air.com.parkerstech.day/cache/data/user/0/air.com.parkerstech.day/no\_backup/androidx.work.workdb.lck data/data/air.com.parkerstech.day/com.parkerstech.day/Local Store/nomo.dat data/data/air.com.parkerstech.day/databases/com.google.android.datatransport.events-journal data/data/air.com.parkerstech.day/databases/google\_app\_measurement\_local.db-journal data/data/air.com.parkerstech.day/databases/OneSignal.db-journal data/data/air.com.parkerstech.day/files/.com.google.firebase.crashlytics.files.v2:air.com.parkerstech.day/com.crashlytics.settings.json data/data/air.com.parkerstech.day/files/.com.google.firebase.crashlytics.files.v2:air.com.parkerstech.day/open-sessions/6746515800460001195AC7F485061D71/report

Showing 1 to 10 of 19 entries



© 2024 Mobile Security Framework - MobSF | <u>Ajin Abraham</u> | <u>OpenSecurity.</u>

Version v4.2.5