MOBSF

ANDROID STATIC ANALYSIS REPORT

OONI Probe (5.1.0)

File Name:	org.openobservatory.ooniprobe_214.apk
Package Name:	org.openobservatory.ooniprobe
Scan Date:	July 31, 2025, 11:08 p.m.

App Security Score: 51/100 (MEDIUM RISK)

Grade: B

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
1	10	2	1	1

FILE INFORMATION

File Name: org.openobservatory.ooniprobe_214.apk
Size: 72.26MB
MD5: 5c09e40db859d610289c9043e18f460f
SHA1: 879887d8a796093050b5787596256a022d0a6f8d

SHA256: c7d7f39a69af7c69ee8f4d370bbd87b6a395e9835616cfeac17d924aba6c693b

APP INFORMATION

App Name: OONI Probe
Package Name: org.openobservatory.ooniprobe
Main Activity: org.ooni.probe.MainActivity
Target SDK: 36
Min SDK: 24
Max SDK:
Android Version Name: 5.1.0
Android Version Code: 214

APP COMPONENTS

Activities: 1
Services: 4
Receivers: 9
Providers: 4
Exported Activities: 2
Exported Services: 1
Exported Receivers: 2
Exported Providers: 0

CERTIFICATE INFORMATION

Binary is signed
v1 signature: False
v2 signature: True
v3 signature: True
v4 signature: False
X.509 Subject: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-04-27 05:36:58+00:00
Valid To: 2044-09-12 05:36:58+00:00
Issuer: C=UK, ST=ORG, L=ORG, O=fdroid.org, OU=FDroid, CN=FDroid
Serial Number: 0x56edccf6
Hash Algorithm: sha256
md5: 0941ac2645a029e5aa4d35b5a39db367
sha1: fc85098c1ec26016541dd0f672ef6bc597ba3b5d
sha256: ceb39f9f7950a5fe84dc917ad3433d146355c861f7f3294ce82d55fb8cb0c0e6
sha512: 68f0ee51e0764596140f4af14333771432b16ce922cdbf4e035e3e99124db83d04574cd1039d264c79ba1ee891a834dbebec22d273aab827bcd056c560562299
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 40e50574878b077dfc87551b04f5a7f8442d55bd205d8bf15d6abb7173606e15
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.FOREGROUND_SERVICE	normal	enables regular apps to use Service.startForeground.	Allows a regular application to use Service.startForeground.
android.permission.FOREGROUND_SERVICE_DATA_SYNC	normal	permits foreground services for data synchronization.	Allows a regular application to use Service.startForeground with the type "dataSync".
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	normal	permission for using Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.	Permission an application must hold in order to use Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.RECEIVE_BOOT_COMPLETED	normal	automatically start at boot	Allows an application to start itself as soon as the system has finished booting. This can make it take longer to start the phone and allow the application to slow down the overall phone by always running.
org.openobservatory.ooniprobe.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Compiler — DETAILS: r8 without marker (suspicious)
classes2.dex	FINDINGS: Compiler — DETAILS: unknown (please file detection issue!)

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes3.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes4.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
<tr><td>classes5.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.MANUFACTURER check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
org.ooni.probe.OONIRunActivity	Schemes: https://, ooni://, Hosts: @string/run_v2_domain, runv2, Path Prefixes: /v2,

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 0 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate

MANIFEST ANALYSIS

HIGH: **1** | WARNING: **6** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable unpatched Android version Android 7.0, [minSdk=24]	high	This application can be installed on an older version of android that has multiple unfixed vulnerabilities. These devices won't receive reasonable security updates from Google. Support an Android version => 10, API 29 to receive reasonable security updates.
2	Application Data can be Backed up [android:allowBackup=true]	warning	This flag allows anyone to backup your application data via adb. It allows users who have enabled USB debugging to copy application data off of the device.
3	Activity-Alias (org.ooni.probe.ShareRunActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
4	Activity-Alias (org.ooni.probe.OONIRunActivity) is not Protected. [android:exported=true]	warning	An Activity-Alias is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device.
5	Service (androidx.work.impl.background.systemjob.SystemJobService) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.BIND_JOB_SERVICE [android:exported=true]	warning	A Service is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
6	Broadcast Receiver (androidx.work.impl.diagnostics.DiagnosticsReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.
7	Broadcast Receiver (androidx.profileinstaller.ProfileInstallReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: android.permission.DUMP [android:exported=true]	warning	A Broadcast Receiver is found to be shared with other apps on the device therefore leaving it accessible to any other application on the device. It is protected by a permission which is not defined in the analysed application. As a result, the protection level of the permission should be checked where it is defined. If it is set to normal or dangerous, a malicious application can request and obtain the permission and interact with the component. If it is set to signature, only applications signed with the same certificate can obtain the permission.

CODE ANALYSIS

HIGH: **0** | WARNING: **3** | INFO: **2** | SECURE: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
1	The App logs information. Sensitive information should never be logged.	info	CWE: CWE-532: Insertion of Sensitive Information into Log File OWASP MASVS: MSTG-STORAGE-3	co/touchlab/kermit/CommonWriter.java co/touchlab/kermit/LogcatWriter.java com/kdroid/androidcontextprovider/ContextInitProvider.java com/kdroid/androidcontextprovider/ContextProvider.java com/mikepenz/markdown/annotator/AnnotatorSettingsKt.java com/multiplatform/webview/util/InternalStoragePathHandler.java io/github/alexzhirkevich/compottie/LottieLogger.java io/github/alexzhirkevich/compottie/LottiePainter.java io/github/alexzhirkevich/compottie/internal/animation/expressions/ExpressionInterpreterImpl.java io/github/alexzhirkevich/compottie/internal/animation/expressions/operations/OpGlobalContext.java org/jetbrains/compose/resources/ResourceReader_androidKt$getPlatformResourceReader$1.java org/jetbrains/skiko/DefaultConsoleLogger.java org/jetbrains/skiko/FPSCounter.java
2	Files may contain hardcoded sensitive information like usernames, passwords, keys etc.	warning	CWE: CWE-312: Cleartext Storage of Sensitive Information OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	com/mikepenz/markdown/compose/elements/MarkdownListKt.java org/ooni/engine/models/TaskEventResult.java org/ooni/engine/models/TestType.java org/ooni/probe/data/models/ResultModel.java org/ooni/probe/data/models/SettingsItem.java org/ooni/probe/ui/navigation/Screen.java org/ooni/probe/ui/settings/category/SettingsCategoryViewModel.java
3	This App uses SQL Cipher. Ensure that secrets are not hardcoded in code.	info	OWASP MASVS: MSTG-CRYPTO-1	app/cash/sqldelight/driver/android/AndroidSqliteDriver.java
4	App creates temp file. Sensitive information should never be written into a temp file.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	org/jetbrains/skiko/Library.java
5	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	org/jetbrains/skiko/Version.java

SHARED LIBRARY BINARY ANALYSIS

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
1	x86_64/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
2	x86_64/libgojni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlcpy_chk', '__memcpy_chk', '__strlen_chk', '__strchr_chk', '__strrchr_chk', '__strlcat_chk', '__memset_chk', '__read_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__memmove_chk', '__strncpy_chk']	True info Symbols are stripped.
3	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NO	SHARED OBJECT	NX	PIE	STACK CANARY	RELRO	RPATH	RUNPATH	FORTIFY	SYMBOLS STRIPPED
4	x86_64/libdatastore_shared_counter.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.
5	x86_64/libgojni.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	True info The binary has the following fortified functions: ['__strlcpy_chk', '__memcpy_chk', '__strlen_chk', '__strchr_chk', '__strrchr_chk', '__strlcat_chk', '__memset_chk', '__read_chk', '__FD_SET_chk', '__FD_CLR_chk', '__FD_ISSET_chk', '__memmove_chk', '__strncpy_chk']	True info Symbols are stripped.
6	x86_64/libandroidx.graphics.path.so	True info The binary has NX bit set. This marks a memory page non-executable making attacker injected shellcode non-executable.	Dynamic Shared Object (DSO) info The shared object is build with -fPIC flag which enables Position independent code. This makes Return Oriented Programming (ROP) attacks much more difficult to execute reliably.	True info This binary has a stack canary value added to the stack so that it will be overwritten by a stack buffer that overflows the return address. This allows detection of overflows by verifying the integrity of the canary before function return.	Full RELRO info This shared object has full RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In Full RELRO, the entire GOT (.got and .got.plt both) is marked as read-only.	None info The binary does not have run-time search path or RPATH set.	None info The binary does not have RUNPATH set.	False warning The binary does not have any fortified functions. Fortified functions provides buffer overflow checks against glibc's commons insecure functions like strcpy, gets etc. Use the compiler option -D_FORTIFY_SOURCE=2 to fortify functions. This check is not applicable for Dart/Flutter libraries.	True info Symbols are stripped.

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	com/multiplatform/webview/util/InternalStoragePathHandler.java okio/Okio__JvmOkioKt.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	org/ooni/probe/AndroidApplication.java org/ooni/probe/MainActivity.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	org/ooni/probe/MainActivity.java
00036	Get resource file from res/raw directory	reflection	org/ooni/probe/AndroidApplication.java org/ooni/probe/MainActivity.java
00022	Open a file from given absolute path of the file	file	org/jetbrains/skiko/Library.java org/ooni/probe/AndroidApplication.java
00028	Read file from assets directory	file	org/jetbrains/compose/resources/ResourceReader_androidKt$getPlatformResourceReader$1.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	4/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.WAKE_LOCK, android.permission.RECEIVE_BOOT_COMPLETED
Other Common Permissions	2/44	android.permission.FOREGROUND_SERVICE, android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS

Malware Permissions:
Top permissions that are widely abused by known malware.

Other Common Permissions:
Permissions that are commonly abused by known malware.

OFAC SANCTIONED COUNTRIES

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

DOMAIN	COUNTRY/REGION

DOMAIN MALWARE CHECK

DOMAIN	STATUS	GEOLOCATION
run.ooni.org	ok	**IP:** 76.76.21.93 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
blog.torproject.org	ok	**IP:** 95.216.163.36 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
github.com	ok	**IP:** 20.26.156.215 **Country:** United States of America **Region:** Washington **City:** Redmond **Latitude:** 47.682899 **Longitude:** -122.120903 **View:** Google Map
schemas.android.com	ok	No Geolocation information available.
explorer.ooni.org	ok	**IP:** 76.76.21.93 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
2019.www.torproject.org	ok	**IP:** 95.216.163.36 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
bridges.torproject.org	ok	**IP:** 116.202.120.184 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map
www.google.comwww.mit.eduwww.yahoo.comwww.slashdot.org	ok	**IP:** 104.18.4.215 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
api.ooni.org	ok	**IP:** 52.59.59.215 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
ooni.org	ok	**IP:** 76.76.21.21 **Country:** United States of America **Region:** California **City:** Walnut **Latitude:** 34.015400 **Longitude:** -117.858223 **View:** Google Map
support.torproject.org	ok	**IP:** 95.216.163.36 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
bugs.torproject.org	ok	**IP:** 95.216.163.36 **Country:** Germany **Region:** Bayern **City:** Nuremberg **Latitude:** 49.447781 **Longitude:** 11.068330 **View:** Google Map
freehaven.net	ok	**IP:** 128.31.0.34 **Country:** United States of America **Region:** Massachusetts **City:** Cambridge **Latitude:** 42.365078 **Longitude:** -71.104523 **View:** Google Map
o155150.ingest.sentry.io	ok	**IP:** 34.120.195.249 **Country:** United States of America **Region:** Missouri **City:** Kansas City **Latitude:** 39.099731 **Longitude:** -94.578568 **View:** Google Map
www.torproject.org	ok	**IP:** 116.202.120.166 **Country:** Germany **Region:** Bayern **City:** Gunzenhausen **Latitude:** 48.323330 **Longitude:** 11.601220 **View:** Google Map

EMAILS

EMAIL	FILE
b9b69705d1ac2c032c69@o155150.ingest	org/ooni/probe/AndroidApplication.java
tor-relays@lists.torproject sa-sha2-256-cert-v01@openssh.comrsa appro@openssl.org -sha2-512-cert-v01@openssh.comssh -ecdsa-sha2-nistp256@openssh.comdiffie	apktool_out/lib/x86_64/libgojni.so

EMAIL	FILE
tor-relays@lists.torproject sa-sha2-256-cert-v01@openssh.comrsa appro@openssl.org -sha2-512-cert-v01@openssh.comssh -ecdsa-sha2-nistp256@openssh.comdiffie	lib/x86_64/libgojni.so

HARDCODED SECRETS

POSSIBLE SECRETS
a-95ed6082-b8e9-46e8-a73f-ff56f00f5d9d
7a49ffedcb48b9b69705d1ac2c032c69
86254750241babac4b8d52996a675549
1cbd3130fa23b59692c061c594c16cc0

PLAYSTORE INFORMATION

Title: OONI Probe

Score: 4.5 **Installs:** 500,000+ **Price:** 0 **Android Version Support:** **Category:** Tools **Play Store URL:** org.openobservatory.ooniprobe

Developer Details: The Tor Project, The+Tor+Project, None, https://ooni.org/, contact@openobservatory.org,

Release Date: Feb 8, 2017 **Privacy Policy:** Privacy link

Description:

Are websites and social media apps blocked? Is your network unusually slow? Run OONI Probe to find out! With this app, you will examine the blocking of websites and instant messaging apps, measure your network's speed and performance, and check whether systems that could be responsible for censorship and surveillance are in your network. OONI Probe is developed by the Open Observatory of Network Interference (OONI), a free software project (under The Tor Project) that aims to uncover internet censorship around the world. Since 2012, OONI's global community has collected millions of network measurements from more than 200 countries, shedding light on multiple cases of network interference. Collect evidence of internet censorship You can check whether and how websites and instant messaging apps are blocked. The network measurement data you will collect may serve as evidence of internet censorship. Detect systems responsible for censorship and surveillance OONI Probe tests are also designed to uncover the presence of systems (middleboxes) that could be responsible for censorship and surveillance. Measure the speed and performance of your network You can measure the speed and performance of your network by running OONI's implementation of the Network Diagnostic Test (NDT). You can also measure video streaming performance with the Dynamic Adaptive Streaming over HTTP (DASH) test. Open data OONI publishes network measurement data because open data allows third parties to verify OONI findings, conduct independent studies, and answer other research questions. Openly publishing OONI data also helps increase transparency of internet censorship around the world. You can explore and download OONI data here: https://ooni.io/data/ Free software All OONI Probe tests (including our NDT and DASH implementations), are based on free and open source software. You can find OONI software projects on GitHub: https://github.com/ooni. Curious to learn how OONI Probe tests work? Learn more: https://ooni.io/nettest/ To receive updates from the OONI-verse, follow us on Twitter: https://twitter.com/OpenObservatory

SCAN LOGS

Timestamp	Event	Error
2025-07-31 23:08:52	Generating Hashes	OK
2025-07-31 23:08:53	Extracting APK	OK
2025-07-31 23:08:53	Unzipping	OK
2025-07-31 23:08:54	Parsing APK with androguard	OK
2025-07-31 23:08:54	Extracting APK features using aapt/aapt2	OK
2025-07-31 23:08:55	Getting Hardcoded Certificates/Keystores	OK
2025-07-31 23:09:04	Parsing AndroidManifest.xml	OK
2025-07-31 23:09:04	Extracting Manifest Data	OK
2025-07-31 23:09:04	Manifest Analysis Started	OK
2025-07-31 23:09:04	Performing Static Analysis on: OONI Probe (org.openobservatory.ooniprobe)	OK
2025-07-31 23:09:05	Fetching Details from Play Store: org.openobservatory.ooniprobe	OK
2025-07-31 23:09:06	Checking for Malware Permissions	OK
2025-07-31 23:09:06	Fetching icon path	OK
2025-07-31 23:09:06	Library Binary Analysis Started	OK

2025-07-31 23:09:06	Analyzing apktool_out/lib/x86_64/libdatastore_shared_counter.so	OK
2025-07-31 23:09:06	Analyzing apktool_out/lib/x86_64/libgojni.so	OK
2025-07-31 23:09:07	Analyzing apktool_out/lib/x86_64/libandroidx.graphics.path.so	OK
2025-07-31 23:09:07	Analyzing lib/x86_64/libdatastore_shared_counter.so	OK
2025-07-31 23:09:07	Analyzing lib/x86_64/libgojni.so	OK
2025-07-31 23:09:08	Analyzing lib/x86_64/libandroidx.graphics.path.so	OK
2025-07-31 23:09:08	Reading Code Signing Certificate	OK
2025-07-31 23:09:10	Running APKiD 2.1.5	OK
2025-07-31 23:09:22	Detecting Trackers	OK
2025-07-31 23:09:34	Decompiling APK to Java with JADX	OK
2025-07-31 23:14:18	Converting DEX to Smali	OK
2025-07-31 23:14:18	Code Analysis Started on - java_source	OK
2025-07-31 23:15:19	Android SBOM Analysis Completed	OK
2025-07-31 23:16:39	Android SAST Completed	OK
2025-07-31 23:16:39	Android API Analysis Started	OK

2025-07-31 23:16:50	Android API Analysis Completed	OK
2025-07-31 23:16:51	Android Permission Mapping Started	OK
2025-07-31 23:17:01	Android Permission Mapping Completed	OK
2025-07-31 23:17:04	Android Behaviour Analysis Started	OK
2025-07-31 23:17:18	Android Behaviour Analysis Completed	OK
2025-07-31 23:17:18	Extracting Emails and URLs from Source Code	OK
2025-07-31 23:17:28	Email and URL Extraction Completed	OK
2025-07-31 23:17:28	Extracting String data from APK	OK
2025-07-31 23:17:28	Extracting String data from SO	OK
2025-07-31 23:17:29	Extracting String data from Code	OK
2025-07-31 23:17:29	Extracting String values and entropies from Code	OK
2025-07-31 23:17:47	Performing Malware check on extracted domains	OK
2025-07-31 23:17:51	Saving to Database	OK