ANDROID STATIC ANALYSIS REPORT

Benefits Pro (1.2.1)

File Name:	com.nb.benefitspro_60.apk
Package Name:	com.nb.benefitspro
Scan Date:	Sept. 1, 2025, 1:06 a.m.
App Security Score:	56/100 (MEDIUM RISK)
Grade:	B
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
2	12	3	3	1

FILE INFORMATION

File Name: com.nb.benefitspro_60.apk
Size: 16.81MB
MD5: ffdee45dc1c4ed0372814c2e301231fe
SHA1: c37ce30f839517dffe2227fe5f4f4c36421ce7d5
SHA256: 88d3d401deecab8d3c7954f8b3e41de364e2346d89ce1b8b07ad0fe268815925

APP INFORMATION

App Name: Benefits Pro
Package Name: com.nb.benefitspro
Main Activity: com.nb.benefitspro.MainActivity
Target SDK: 34
Min SDK: 26
Max SDK:
Android Version Name: 1.2.1

Android Version Code: 60

APP COMPONENTS

Activities: 3
Services: 10
Receivers: 4
Providers: 4
Exported Activities: 0
Exported Services: 0
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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2023-06-09 11:35:00+00:00
Valid To: 2053-06-09 11:35:00+00:00
Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
Serial Number: 0xe653127762f975fa93fe7706618022933677db53
Hash Algorithm: sha256
md5: 198a33c17e8bc87f67ce13aa2cb3ad97
sha1: 1e9d3469d8c597e1ffbc5c4478fcf52bf9005a51
sha256: 8cd6498badc2e630846844d760d5153d764fc57e14db95e19e948345b1c0c9e7
sha512: 9d2cc0c35b36105978b6af4a3ce8eaea8cc975c84f3e5c25fe818f653464e4e94804df5800fb5d7804e30c31b9fa7b25f469eb0c8a50022c10f29c8e703a0fcd
PublicKey Algorithm: rsa
Bit Size: 4096
Fingerprint: e51d46e23bcbef90690bb33c73fdbcaebe2234009fe3d19afcc2c1dce3f60873
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.CAMERA	dangerous	take pictures and videos	Allows application to take pictures and videos with the camera. This allows the application to collect images that the camera is seeing at any time.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_DOWNLOAD_MANAGER	unknown	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_COARSE_LOCATION	dangerous	coarse (network-based) location	Access coarse location sources, such as the mobile network database, to determine an approximate phone location, where available. Malicious applications can use this to determine approximately where you are.
android.permission.ACCESS_FINE_LOCATION	dangerous	fine (GPS) location	Access fine location sources, such as the Global Positioning System on the phone, where available. Malicious applications can use this to determine where you are and may consume additional battery power.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.POST_NOTIFICATIONS	dangerous	allows an app to post notifications.	Allows an app to post notifications
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.
android.permission.USE_BIOMETRIC	normal	allows use of device-supported biometric modalities.	Allows an app to use device supported biometric modalities.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.
com.google.android.gms.permission.AD_ID	normal	application shows advertisements	This app uses a Google advertising ID and can possibly serve advertisements.
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	normal	allow applications to access advertising service attribution	This enables the app to retrieve information related to advertising attribution, which can be used for targeted advertising purposes. App can gather data about how users interact with ads, such as clicks or impressions, to measure the effectiveness of advertising campaigns.

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.ACCESS_ADSERVICES_AD_ID	normal	allow app to access the device's advertising ID.	This ID is a unique, user-resettable identifier provided by Google's advertising services, allowing apps to track user behavior for advertising purposes while maintaining user privacy.
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	normal	permission defined by google	A custom permission defined by Google.
com.nb.benefitspro.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	unknown	Unknown permission	Unknown permission from android reference

APKID ANALYSIS

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>ffdee45dc1c4ed0372814c2e301231fe.apk</td><td><table><tr><th>FINDINGS</th><th>DETAILS</th></tr><tr><td>Anti-VM Code</td><td>possible VM check</td></tr></table></td></tr>
</table>

<table>
<tr><th>FILE</th><th>DETAILS</th></tr>
<tr><td>classes.dex</td><td>
<table>
<tr><th>FINDINGS</th><th>DETAILS</th></tr>
<tr><td>Anti-VM Code</td><td>Build.FINGERPRINT check
Build.MODEL check
Build.MANUFACTURER check
Build.PRODUCT check
Build.HARDWARE check
Build.TAGS check
SIM operator check
network operator name check
device ID check
possible VM check</td></tr>
<tr><td>Anti Debug Code</td><td>Debug.isDebuggerConnected() check</td></tr>
<tr><td>Compiler</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>

BROWSABLE ACTIVITIES

ACTIVITY	INTENT
com.nb.benefitspro.MainActivity	Schemes: nb://, Hosts: nb-prod-otc2-api.nationsbenefits.com,

NETWORK SECURITY

HIGH: **0** | WARNING: **0** | INFO: **0** | SECURE: **0**

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: **0** | WARNING: **4** | INFO: **0** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable Android version Android 8.0, minSdk=26]	warning	This application can be installed on an older version of android that has multiple vulnerabilities. Support an Android version => 10, API 29 to receive reasonable security updates.

NO	ISSUE	SEVERITY	DESCRIPTION
2	App has a Network Security Configuration [android:networkSecurityConfig=@xml/network_security_config]	info	The Network Security Configuration feature lets apps customize their network security settings in a safe, declarative configuration file without modifying app code. These settings can be configured for specific domains and for a specific app.
3	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.
4	Broadcast Receiver (com.google.firebase.iid.FirebaseInstanceIdReceiver) is Protected by a permission, but the protection level of the permission should be checked. Permission: com.google.android.c2dm.permission.SEND [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.
5	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: **2** | WARNING: **6** | INFO: **3** | SECURE: **2** | SUPPRESSED: **0**

NO	ISSUE	SEVERITY	STANDARDS	FILES
				A4/b.java A6/c.java B/g.java B0/e.java C/b.java C1/e.java C6/B.java C6/M.java C8/d.java D2/d.java E1/c.java E1/f.java E1/g.java E1/i.java E1/m.java E4/f.java E4/h.java E6/f.java F2/C0159x.java F2/N.java F2/Y.java F2/d0.java I/f.java I/k.java I/r.java I1/C0238e.java J1/g.java J4/l.java J5/c.java J5/d.java K/a.java K1/n.java L1/i.java L1/l.java M/g.java M1/c.java M4/AbstractC0495y0.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				M4/C6.java M4/C5.java M4/Z4.java M4/c7.java N2/i.java O5/e.java O5/g.java O6/a.java P6/a.java P6/c.java Pg/i.java Q1/n.java Q6/b.java Q6/c.java Q6/o.java Q6/p.java R1/a.java R1/b.java R6/a.java R8/C0745a.java T3/j.java T5/d.java T5/e.java U4/C0943j.java U4/G.java U4/e1.java U4/p1.java U4/v1.java V1/C1028b.java V1/C1034e.java V1/C1049o.java V1/l.java V1/U.java V1/p0.java V1/q0.java V1/v0.java V3/d.java V5/a.java V5/c.java V5/d.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				Vf/m.java W0/C1119x.java W0/O.java W5/b.java W5/c.java W5/d.java W6/k.java X4/a.java X5/c.java Y3/B0.java Y3/M0.java Y3/s0.java Y3/y0.java Y3/z0.java Y5/b.java Y6/d.java Z5/g.java Z5/i.java Z5/m.java Z5/o.java Z5/q.java Z5/r.java Z5/s.java Z5/t.java Z5/v.java Z5/x.java a/RunnableC1348q.java a5/C1405b.java a6/C1410d.java a6/h.java a6/m.java b2/q.java c1/C1689a.java c2/C1702c.java d4/s.java e6/C2188a.java e6/C2189b.java f2/C2287e.java f5/RunnableC2313b.java f6/C2322c.java

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	g/AbstractC2362c.java g/C2363d.java g/HandlerC2366g.java g/k.java g/y.java g/z.java g6/b.java gd/g.java h/RunnableC2485b.java i/C2645i.java i/C2646j.java j/ViewOnKeyListenerC2888i.java j/o.java k/AbstractC3015k0.java k/B1.java k/C3023o0.java k/C3037w.java k/C3039x.java k/C3043z.java k/M0.java k/P.java k/RunnableC3012j.java k/S0.java k/ViewOnClickListenerC2998c.java k/W.java k/m1.java k/n1.java k4/C3070c.java k4/C3076i.java n0/C3329A.java n2/C3340b.java n3/a.java n5/C3355c.java o/G.java o/o.java o/r.java o/u.java o0/f1.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				o2/C3628b.java o2/C3629c.java o2/C3633g.java o5/AbstractC3647a.java p4/C3737a.java q2/AbstractComponentCallbacksC3866q.java q2/AnimationAnimationListenerC3854e.java q2/C3841E.java q2/C3844H.java q2/C3847K.java q2/C3850a.java q2/C3853d.java q2/C3858i.java q2/DialogInterfaceOnCancelListenerC3862m.java q2/LayoutInflaterFactory2C3871w.java q2/W.java q2/Y.java q2/Z.java q3/b.java q5/e.java q5/g.java r2/c.java r4/AbstractC3964l.java r4/C3954b.java r4/C3955c.java r4/C3958f.java r4/C3965m.java r4/HandlerC3957e.java r4/RunnableC3960h.java s/C4106m0.java s/C4108n0.java s/RunnableC4064O0.java s4/C4150e.java s4/C4151f.java s4/i.java s4/l.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
				s4/o.java s4/s.java sh/l.java t3/C4254d.java u1/C4353d.java u3/k.java u4/C4373e.java u4/C4389u.java u4/RunnableC4387s.java u6/b.java v4/AbstractC4473e.java v4/AbstractC4490w.java v4/C4477i.java v4/C4483o.java v4/J.java v4/K.java v4/Q.java v4/z.java w5/e.java x/C4598c.java x5/f.java x5/i.java x5/k.java y1/d.java y2/AbstractC4756q.java y2/C4754o.java y3/C4763c.java y6/AbstractC4778e.java y6/BinderC4771C.java y6/RunnableC4769A.java y6/ServiceConnectionC4773E.java y6/g.java y6/j.java y6/n.java y6/o.java y6/s.java y6/t.java y6/u.java y6/v.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	SHA-1 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	Z5/g.java k/C3037w.java u6/b.java
3	App uses SQLite Database and execute raw SQL query. Untrusted user input in raw SQL queries can cause SQL Injection. Also sensitive information should be encrypted and written to the database.	warning	CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') OWASP Top 10: M7: Client Code Quality	l/f.java M4/AbstractC0349f5.java U4/C0941i.java U4/E.java U4/p1.java U4/y1.java U5/h.java V5/c.java k4/C3070c.java k4/C3075h.java k4/C3076i.java l4/C3182h.java l4/C3188n.java s/C4095h.java
4	The App uses an insecure Random Number Generator.	warning	CWE: CWE-330: Use of Insufficiently Random Values OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	B/f.java F3/k.java M/g.java P5/b.java Sg/a.java Tg/a.java U4/v1.java W3/d.java xh/g.java
5	The App uses the encryption mode CBC with PKCS5/PKCS7 padding. This configuration is vulnerable to padding oracle attacks.	high	CWE: CWE-649: Reliance on Obfuscation or Encryption of Security-Relevant Inputs without Integrity Checking OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-3	M4/c7.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
6	This App copies data to clipboard. Sensitive data should not be copied to clipboard as other applications can access it.	info	OWASP MASVS: MSTG-STORAGE-10	T/U.java
7	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	sh/d.java sh/g.java sh/l.java
8	This App may have root detection capabilities.	secure	OWASP MASVS: MSTG-RESILIENCE-1	Z5/g.java w5/e.java
9	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	H3/c.java Ud/C0979d.java W2/c.java a6/C1408b.java b6/C1573g0.java gb/b.java wa/C4581a.java
10	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	U4/e1.java
11	The file or SharedPreference is World Writable. Any App can write to the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	m8/u.java
12	App can write to App Directory. Sensitive Information should be encrypted.	info	CWE: CWE-276: Incorrect Default Permissions OWASP MASVS: MSTG-STORAGE-14	w3/C4561f.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
13	MD5 is a weak hash known to have hash collisions.	warning	CWE: CWE-327: Use of a Broken or Risky Cryptographic Algorithm OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	U4/v1.java

NIAP ANALYSIS v1.3

NO	IDENTIFIER	REQUIREMENT	FEATURE	DESCRIPTION

BEHAVIOUR ANALYSIS

RULE ID	BEHAVIOUR	LABEL	FILES
00108	Read the input stream from given URL	network command	U4/G0.java U4/N.java
00009	Put data in cursor to JSON object	file	A6/c.java

RULE ID	BEHAVIOUR	LABEL	FILES
00013	Read file and put it into a stream	file	C8/c.java D2/a.java D2/d.java D2/i.java F3/k.java H3/a.java M1/c.java U4/e1.java Z5/g.java Z5/o.java a6/h.java e6/C2188a.java g6/b.java o2/C3633g.java yh/w.java
00191	Get messages in the SMS inbox	sms	k/m1.java
00036	Get resource file from res/raw directory	reflection	M4/Y4.java N2/c.java U4/C0943j.java k/m1.java s4/C4151f.java
00022	Open a file from given absolute path of the file	file	H3/a.java Q2/a.java a6/h.java d3/AbstractC2092f.java w3/C4561f.java

RULE ID	BEHAVIOUR	LABEL	FILES
00063	Implicit intent(view a web page, make a phone call, etc.)	control	M4/Y4.java U4/C0943j.java U4/v1.java c1/C1689a.java f0/z0.java q2/RunnableC3855f.java s4/C4151f.java y2/AbstractC4756q.java
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	M4/Y4.java U4/C0943j.java f0/z0.java s4/C4151f.java
00094	Connect to a URL and read data from it	command network	U4/C0943j.java
00109	Connect to a URL and get the response code	network command	U4/I0.java V5/c.java t3/C4254d.java
00162	Create InetSocketAddress object and connecting to it	socket	sh/l.java
00163	Create new Socket and connecting to it	socket	sh/l.java
00075	Get location of the device	collection location	g/C2363d.java
00137	Get last known location of the device	location collection	g/C2363d.java

RULE ID	BEHAVIOUR	LABEL	FILES
00014	Read file into a stream and put it into a JSON object	file	F3/k.java U4/e1.java a6/h.java g6/b.java
00005	Get absolute path of file and put it to JSON object	file	a6/h.java w3/C4561f.java
00030	Connect to the remote server through the given URL	network	U4/I0.java
00114	Create a secure socket connection to the proxy address	network command	oh/l.java
00024	Write file after Base64 decoding	reflection file	d3/AbstractC2092f.java
00096	Connect to a URL and set request method	command network	Q6/b.java V5/c.java
00089	Connect to a URL and receive input stream from the server	command network	Q6/b.java V5/c.java
00125	Check if the given file path exist	file	V5/c.java
00091	Retrieve data from broadcast	collection	d4/s.java
00012	Read data and put it into a buffer stream	file	o2/C3633g.java

FIREBASE DATABASES ANALYSIS

TITLE	SEVERITY	DESCRIPTION
Firebase Remote Config disabled	secure	Firebase Remote Config is disabled for https://firebaseremoteconfig.googleapis.com/v1/projects/648213817563/namespaces/firebase:fetch?key=AIzaSyAirb5vvRVSXzYXGgQRv5dQWWblxWrxUiw. This is indicated by the response: {'state': 'NO_TEMPLATE'}

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	7/25	android.permission.INTERNET, android.permission.ACCESS_NETWORK_STATE, android.permission.CAMERA, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_COARSE_LOCATION, android.permission.ACCESS_FINE_LOCATION, android.permission.WAKE_LOCK
Other Common Permissions	3/44	com.google.android.c2dm.permission.RECEIVE, com.google.android.gms.permission.AD_ID, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE

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
nb-prod-otc2-api.nationsbenefits.com	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
api.eu.amplitude.com	ok	**IP:** 18.196.51.99 **Country:** Germany **Region:** Hessen **City:** Frankfurt am Main **Latitude:** 50.115520 **Longitude:** 8.684170 **View:** Google Map
xml.org	ok	**IP:** 104.239.142.8 **Country:** United States of America **Region:** Texas **City:** Windcrest **Latitude:** 29.499678 **Longitude:** -98.399246 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
issuetracker.google.com	ok	**IP:** 142.250.201.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.w3.org	ok	**IP:** 104.18.23.19 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
nationscdn.azureedge.net	ok	**IP:** 13.107.246.71 **Country:** Netherlands **Region:** Noord-Holland **City:** Amsterdam **Latitude:** 52.374031 **Longitude:** 4.889690 **View:** Google Map
firebase.google.com	ok	**IP:** 142.250.179.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
developer.android.com	ok	**IP:** 142.250.72.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
www.google.com	ok	**IP:** 172.217.20.164 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
app-measurement.com	ok	**IP:** 142.250.201.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
pagead2.googlesyndication.com	ok	**IP:** 142.250.178.130 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
api2.amplitude.com	ok	**IP:** 52.33.55.240 **Country:** United States of America **Region:** Oregon **City:** Portland **Latitude:** 45.523449 **Longitude:** -122.676208 **View:** Google Map
goo.gl	ok	**IP:** 142.250.201.174 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
picsum.photos	ok	**IP:** 104.26.4.30 **Country:** United States of America **Region:** California **City:** San Francisco **Latitude:** 37.775700 **Longitude:** -122.395203 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
nationsmarket.co	ok	**IP:** 148.72.48.1 **Country:** United States of America **Region:** Arizona **City:** Scottsdale **Latitude:** 33.601974 **Longitude:** -111.887917 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.docs.developers.amplitude.com	ok	**IP:** 66.33.60.67 **Country:** Canada **Region:** Ontario **City:** Etobicoke **Latitude:** 43.623768 **Longitude:** -79.559723 **View:** Google Map
firebase-settings.crashlytics.com	ok	**IP:** 216.58.213.67 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map
order-tracking.com	ok	**IP:** 8.208.21.37 **Country:** United Kingdom of Great Britain and Northern Ireland **Region:** England **City:** London **Latitude:** 51.508530 **Longitude:** -0.125740 **View:** Google Map
google.com	ok	**IP:** 216.58.213.78 **Country:** United States of America **Region:** California **City:** Mountain View **Latitude:** 37.405991 **Longitude:** -122.078514 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
xmlpull.org	ok	**IP:** 185.199.110.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map
www.instacart.com	ok	**IP:** 172.64.150.189 **Country:** United States of America **Region:** Texas **City:** Dallas **Latitude:** 32.783058 **Longitude:** -96.806671 **View:** Google Map
goo.gle	ok	**IP:** 67.199.248.13 **Country:** United States of America **Region:** New York **City:** New York City **Latitude:** 40.739288 **Longitude:** -73.984955 **View:** Google Map

✉ EMAILS

EMAIL	FILE
example@email.com	pa/f.java

EMAIL	FILE
example@email.com	Oc/a.java
u0013android@android.com0 u0013android@android.com	s4/q.java

TRACKERS

TRACKER	CATEGORIES	URL
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

HARDCODED SECRETS

POSSIBLE SECRETS
"com.google.firebase.crashlytics.mapping_file_id" : "3a21240b01ec481688690ac3ca7863f5"
"google_api_key" : "AIzaSyAirb5vvRVSXzYXGgQRv5dQWWblxWrxUiw"
"google_crash_reporting_api_key" : "AIzaSyAirb5vvRVSXzYXGgQRv5dQWWblxWrxUiw"
edef8ba9-79d6-4ace-a3c8-27dcd51d21ed

POSSIBLE SECRETS
9e03a8041e6a48c2f464891b5318e826
258EAFA5-E914-47DA-95CA-C5AB0DC85B11
470fa2b4ae81cd56ecbcda9735803434cec591fa

PLAYSTORE INFORMATION

Title: Benefits Pro

Score: 4.50603 **Installs:** 100,000+ **Price:** 0 **Android Version Support:** **Category:** Health & Fitness **Play Store URL:** com.nb.benefitspro

Developer Details: NationsBenefits, LLC, NationsBenefits,+LLC, None, https://www.nationsbenefits.com/, appsupport@nationsbenefits.com,

Release Date: Aug 31, 2023 **Privacy Policy:** Privacy link

Description:

The Benefits Pro mobile app is an all-in-one solution that gives members access to all of their benefits in one place. The app offers a world-class experience designed to improve health outcomes, decrease healthcare spending, and increase member satisfaction. Download the app and enjoy easy access to shopping, benefit information, transaction history, and more. The Benefits Pro app allows you to filter, sort, and search by category, pricing, wallet, and more. See products in more detail with 360-degree expandable images. You can easily access benefit tracking to see available dollars to spend on plan-approved products to live a healthier lifestyle. All orders are shipped with nationwide 2-day delivery at no additional cost.

SCAN LOGS

Timestamp	Event	Error
2025-09-01 01:06:27	Generating Hashes	OK

2025-09-01 01:06:28	Extracting APK	OK
2025-09-01 01:06:28	Unzipping	OK
2025-09-01 01:06:31	Parsing APK with androguard	OK
2025-09-01 01:06:31	Extracting APK features using aapt/aapt2	OK
2025-09-01 01:06:31	Getting Hardcoded Certificates/Keystores	OK
2025-09-01 01:06:33	Parsing AndroidManifest.xml	OK
2025-09-01 01:06:33	Extracting Manifest Data	OK
2025-09-01 01:06:33	Manifest Analysis Started	OK
2025-09-01 01:06:33	Reading Network Security config from network_security_config.xml	OK
2025-09-01 01:06:33	Parsing Network Security config	OK

2025-09-01 01:06:33	Performing Static Analysis on: Benefits Pro (com.nb.benefitspro)	OK
2025-09-01 01:06:37	Fetching Details from Play Store: com.nb.benefitspro	OK
2025-09-01 01:06:39	Checking for Malware Permissions	OK
2025-09-01 01:06:39	Fetching icon path	OK
2025-09-01 01:06:39	Library Binary Analysis Started	OK
2025-09-01 01:06:41	Reading Code Signing Certificate	OK
2025-09-01 01:06:42	Running APKiD 2.1.5	OK
2025-09-01 01:06:45	Detecting Trackers	OK
2025-09-01 01:06:50	Decompiling APK to Java with JADX	OK
2025-09-01 01:07:22	Decompiling with JADX failed, attempting on all DEX files	OK

2025-09-01 01:07:23	Decompiling classes.dex with JADX	OK
2025-09-01 01:25:04	Decompiling with JADX timed out	TimeoutExpired(['/home/mobsf/.MobSF/tools/jadx/jadx-1.5.0/bin/jadx', '-ds', '/home/mobsf/.MobSF/uploads/ffdee45dc1c4ed0372814c2e301231fe/java_source', '-q', '-r', '--show-bad-code', '/home/mobsf/.MobSF/uploads/ffdee45dc1c4ed0372814c2e301231fe/classes.dex'], 999.9997878670692)
2025-09-01 01:25:04	Converting DEX to Smali	OK
2025-09-01 01:25:04	Code Analysis Started on - java_source	OK
2025-09-01 01:25:14	Android SBOM Analysis Completed	OK
2025-09-01 01:25:27	Android SAST Completed	OK
2025-09-01 01:25:27	Android API Analysis Started	OK
2025-09-01 01:25:41	Android API Analysis Completed	OK
2025-09-01 01:25:42	Android Permission Mapping Started	OK
2025-09-01 01:25:53	Android Permission Mapping Completed	OK

2025-09-01 01:25:54	Android Behaviour Analysis Started	OK
2025-09-01 01:26:06	Android Behaviour Analysis Completed	OK
2025-09-01 01:26:06	Extracting Emails and URLs from Source Code	OK
2025-09-01 01:26:11	Email and URL Extraction Completed	OK
2025-09-01 01:26:11	Extracting String data from APK	OK
2025-09-01 01:26:11	Extracting String data from Code	OK
2025-09-01 01:26:11	Extracting String values and entropies from Code	OK
2025-09-01 01:26:15	Performing Malware check on extracted domains	OK
2025-09-01 01:26:23	Saving to Database	OK

Report Generated by - MobSF v4.4.0

Mobile Security Framework (MobSF) is an automated, all-in-one mobile application (Android/iOS/Windows) pen-testing, malware analysis and security assessment framework capable of performing static and dynamic analysis.