MOBSF

ANDROID STATIC ANALYSIS REPORT

nomo (5.1.141)

File Name:	nomo - Sobriety Clocks_5.1.141_APKPure.apk
Package Name:	air.com.parkerstech.day
Scan Date:	Nov. 23, 2024, 8:01 p.m.
App Security Score:	35/100 (HIGH RISK)
Grade:	C
Trackers Detection:	2/432

FINDINGS SEVERITY

HIGH	MEDIUM	INFO	SECURE	HOTSPOT
7	11	1	1	1

FILE INFORMATION

File Name: nomo - Sobriety Clocks_5.1.141_APKPure.apk
Size: 22.05MB
MD5: 35320518c6146dc9fb10b987269bc5a6
SHA1: 97b0355df44d1cd69cdb1bc5a42b4658f846eccc
SHA256: ed561826bc36a9d75274f1da33d8b061e70a6447b3cbb156e6bf54015206cfc2

APP INFORMATION

App Name: nomo
Package Name: air.com.parkerstech.day
Main Activity: .AppEntry
Target SDK: 26
Min SDK: 9
Max SDK:
Android Version Name: 5.1.141
Android Version Code: 500001141

APP COMPONENTS

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

CERTIFICATE INFORMATION

Binary is signed
v1 signature: True
v2 signature: False
v3 signature: False
v4 signature: False
X.509 Subject: C=US, O=Nomo, OU=Nomo, CN=Parker Stech
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2016-05-19 17:40:59+00:00
Valid To: 2041-05-20 17:40:59+00:00
Issuer: C=US, O=Nomo, OU=Nomo, CN=Parker Stech
Serial Number: 0x37353638666165623a3135346366343138393339 3a2d38303030
Hash Algorithm: sha1
md5: f8ff2da9aab8dc5743f415d8434858b0
sha1: ceca156649ea79d9f88202299efba651510fc4fa
sha256: ff2d0913f5ca7be33ed9b988bb2d026bb67b5f2296708a632dbd91b27f889732
sha512: e83ba43ba9c8e1aa3066e95a2ab2375c5ed97dbc0f22d95615593b501127f40e34ddc3fa7e1940d75f8e9f4bc7f97290e5b11bc944bfdee016356963829bf6c2
Found 1 unique certificates

APPLICATION PERMISSIONS

PERMISSION	STATUS	INFO	DESCRIPTION
android.permission.READ_PHONE_STATE	dangerous	read phone state and identity	Allows the application to access the phone features of the device. An application with this permission can determine the phone number and serial number of this phone, whether a call is active, the number that call is connected to and so on.
android.permission.GET_ACCOUNTS	dangerous	list accounts	Allows access to the list of accounts in the Accounts Service.
android.permission.GET_TASKS	dangerous	retrieve running applications	Allows application to retrieve information about currently and recently running tasks. May allow malicious applications to discover private information about other applications.
android.permission.WAKE_LOCK	normal	prevent phone from sleeping	Allows an application to prevent the phone from going to sleep.
android.permission.VIBRATE	normal	control vibrator	Allows the application to control the vibrator.
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.INTERNET	normal	full Internet access	Allows an application to create network sockets.
android.permission.WRITE_EXTERNAL_STORAGE	dangerous	read/modify/delete external storage contents	Allows an application to write to external storage.
android.permission.ACCESS_NETWORK_STATE	normal	view network status	Allows an application to view the status of all networks.
android.permission.ACCESS_WIFI_STATE	normal	view Wi-Fi status	Allows an application to view the information about the status of Wi-Fi.
android.permission.USE_FINGERPRINT	normal	allow use of fingerprint	This constant was deprecated in API level 28. Applications should request USE_BIOMETRIC instead.

PERMISSION	STATUS	INFO	DESCRIPTION
air.com.parkerstech.day.permission.C2D_MESSAGE	unknown	Unknown permission	Unknown permission from android reference
com.google.android.c2dm.permission.RECEIVE	normal	recieve push notifications	Allows an application to receive push notifications from cloud.

APKID ANALYSIS

FILE	DETAILS
classes.dex	FINDINGS: Anti-VM Code — DETAILS: Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check device ID check possible VM check FINDINGS: Compiler — DETAILS: dexlib 2.x

NETWORK SECURITY

NO	SCOPE	SEVERITY	DESCRIPTION

CERTIFICATE ANALYSIS

HIGH: 2 | WARNING: 0 | INFO: 1

TITLE	SEVERITY	DESCRIPTION
Signed Application	info	Application is signed with a code signing certificate
Application vulnerable to Janus Vulnerability	high	Application is signed with v1 signature scheme, making it vulnerable to Janus vulnerability on Android 5.0-8.0, if signed only with v1 signature scheme. Applications running on Android 5.0-7.0 signed with v1, and v2/v3 scheme is also vulnerable.
Certificate algorithm vulnerable to hash collision	high	Application is signed with SHA1withRSA. SHA1 hash algorithm is known to have collision issues.

MANIFEST ANALYSIS

HIGH: 2 | WARNING: 2 | INFO: 0 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	DESCRIPTION
1	App can be installed on a vulnerable upatched Android version Android 2.3-2.3.2, [minSdk=9]	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] flag is missing.	warning	The flag [android:allowBackup] should be set to false. By default it is set to true and 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.

NO	ISSUE	SEVERITY	DESCRIPTION
3	Launch Mode of activity (.AppEntry) is not standard.	warning	An Activity should not be having the launch mode attribute set to "singleTask/singleInstance" as it becomes root Activity and it is possible for other applications to read the contents of the calling Intent. So it is required to use the "standard" launch mode attribute when sensitive information is included in an Intent.
4	Activity (.AppEntry) is vulnerable to Android Task Hijacking/StrandHogg.	high	An Activity should not be having the launch mode attribute set to "singleTask". It is then possible for other applications to place a malicious activity on top of the activity stack resulting in Task Hijacking/StrandHogg 1.0 vulnerability. This makes the application an easy target for phishing attacks. The vulnerability can be remediated by setting the launch mode attribute to "singleInstance" or by setting an empty taskAffinity (taskAffinity="") attribute. You can also update the target SDK version (26) of the app to 28 or higher to fix this issue at platform level.

</> CODE ANALYSIS

HIGH: 3 | WARNING: 7 | INFO: 1 | SECURE: 1 | SUPPRESSED: 0

NO	ISSUE	SEVERITY	STANDARDS	FILES
				air/com/parkerstech/day/AppEntry.java air/com/parkerstech/day/GetVersionCode.java c/m/x/a/ep/ac.java c/m/x/a/ep/ax.java c/m/x/a/ep/ay.java c/m/x/a/ep/az.java c/m/x/a/ep/ba.java c/m/x/a/ep/bd.java c/m/x/a/ep/be.java c/m/x/a/ep/bj.java c/m/x/a/ep/bk.java c/m/x/a/ep/bl.java c/m/x/a/ep/bm.java c/m/x/a/ep/bo.java com/adobe/air/AndroidGcmRegistrationService.java com/adobe/air/AndroidWebView.java com/adobe/air/GetVersionCode.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	com/adobe/air/microphone/AIRMicrophoneRecorder.java com/adobe/air/utils/AIRLogger.java com/adobe/flashruntime/air/VideoTextureSurface.java com/adobe/flashruntime/shared/VideoView.java com/distriqt/core/utils/LogUtil.java com/distriqt/extension/vibration/VibrationExtension.java com/freshplanet/ane/KeyboardSize/ExtensionContext.java com/freshplanet/ane/KeyboardSize/getKeyboardHeight.java com/freshplanet/ane/KeyboardSize/getKeyboardY.java com/milkmangames/extensions/android/a.java com/milkmangames/extensions/android/b.java com/milkmangames/extensions/android/c.java com/milkmangames/extensions/android/d.java com/milkmangames/extensions/android/e.java com/milkmangames/extensions/android/h.java com/milkmangames/extensions/android/k.java com/milkmangames/extensions/android/l.java com/milkmangames/extensions/android/m.java com/milkmangames/extensions/android/n.java com/milkmangames/extensions/android/push/PushNotifyExtension.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
2	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	com/adobe/air/AdobeAIRMainActivity.java com/distriqt/extension/dialog/dialogview/DialogViewController.java
3	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	com/distriqt/extension/localauth/controller/LocalAuthController.java
4	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	com/distriqt/core/utils/VDK.java com/distriqt/extension/dialog/functions/VDKFunction.java
5	Insecure WebView Implementation. Execution of user controlled code in WebView is a critical Security Hole.	warning	CWE: CWE-749: Exposed Dangerous Method or Function OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/distriqt/extension/nativewebview/controller/NativeWebView.java
6	Ensure that user controlled URLs never reaches the Webview. Enabling file access from URLs in WebView can leak sensitive information from the file system.	warning	CWE: CWE-200: Information Exposure OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	com/adobe/air/AndroidWebView.java com/distriqt/extension/nativewebview/controller/NativeWebView.java
7	IP Address disclosure	warning	CWE: CWE-200: Information Exposure OWASP MASVS: MSTG-CODE-2	com/adobe/air/GetVersionCode.java
8	App can read/write to External Storage. Any App can read data written to External Storage.	warning	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/adobe/air/CameraUI.java com/adobe/air/CameraUIProvider.java com/adobe/air/utils/Utils.java com/distriqt/extension/nativewebview/utils/ContentProviderUtils.java

NO	ISSUE	SEVERITY	STANDARDS	FILES
9	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	com/adobe/air/CameraUI.java
10	The file or SharedPreference is World Readable. Any App can read from the file	high	CWE: CWE-276: Incorrect Default Permissions OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	com/adobe/air/AIRSharedPref.java com/adobe/air/utils/Utils.java
11	This App uses SSL certificate pinning to detect or prevent MITM attacks in secure communication channel.	secure	OWASP MASVS: MSTG-NETWORK-4	com/adobe/air/JavaTrustStoreHelper.java
12	Insecure WebView Implementation. WebView ignores SSL Certificate errors and accept any SSL Certificate. This application is vulnerable to MITM attacks	high	CWE: CWE-295: Improper Certificate Validation OWASP Top 10: M3: Insecure Communication OWASP MASVS: MSTG-NETWORK-3	com/adobe/air/AndroidWebView.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	armeabi-v7a/libysshared.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
2	armeabi-v7a/libCore.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as 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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
3	armeabi-v7a/libc++_shared.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	armeabi-v7a/libysshared.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
5	armeabi-v7a/libCore.so	False high The binary does not have NX bit set. NX bit offer protection against exploitation of memory corruption vulnerabilities by marking memory page as non-executable. Use option --noexecstack or -z noexecstack to mark stack as 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.	Partial RELRO warning This shared object has partial RELRO enabled. RELRO ensures that the GOT cannot be overwritten in vulnerable ELF binaries. In partial RELRO, the non-PLT part of the GOT section is read only but .got.plt is still writeable. Use the option -z,relro,-z,now to enable full RELRO.	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
6	armeabi-v7a/libc++_shared.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
00192	Get messages in the SMS inbox	sms	com/adobe/air/AndroidMediaManager.java com/distriqt/extension/nativewebview/controller/NativeWebView.java com/distriqt/extension/nativewebview/utils/ContentProviderUtils.java
00063	Implicit intent(view a web page, make a phone call, etc.)	control	c/m/x/a/ep/ax.java com/adobe/air/AdobeAIRWebView.java com/adobe/air/AndroidActivityWrapper.java com/adobe/air/AndroidMediaManager.java com/distriqt/extension/nativewebview/controller/NativeWebView.java com/distriqt/extension/nativewebview/controller/browser/BrowserView.java com/distriqt/extension/nativewebview/controller/webview/AdvancedWebView.java com/milkmangames/extensions/android/a.java
00052	Deletes media specified by a content URI(SMS, CALL_LOG, File, etc.)	sms	com/adobe/air/AndroidMediaManager.java
00011	Query data from URI (SMS, CALLLOGS)	sms calllog collection	com/adobe/air/AndroidMediaManager.java com/distriqt/extension/nativewebview/utils/ContentProviderUtils.java

RULE ID	BEHAVIOUR	LABEL	FILES
00022	Open a file from given absolute path of the file	file	c/m/x/a/ep/ar.java c/m/x/a/ep/ax.java com/adobe/air/AndroidActivityWrapper.java com/adobe/air/ApplicationFileManager.java com/adobe/air/CameraUI.java com/adobe/air/DeviceProfiling.java com/adobe/air/Entrypoints.java com/adobe/air/utils/Utils.java com/distriqt/core/utils/Assets.java com/distriqt/core/utils/FREImageUtils.java com/distriqt/core/utils/FileProviderUtils.java com/distriqt/extension/nativewebview/utils/Assets.java
00013	Read file and put it into a stream	file	com/adobe/air/ApplicationFileManager.java com/adobe/air/JavaTrustStoreHelper.java com/adobe/air/utils/Utils.java com/distriqt/core/utils/Assets.java com/distriqt/core/utils/FileProviderUtils.java com/distriqt/extension/nativewebview/utils/Assets.java
00028	Read file from assets directory	file	com/distriqt/core/utils/Assets.java com/distriqt/extension/nativewebview/utils/Assets.java
00102	Set the phone speaker on	command	com/adobe/air/AndroidActivityWrapper.java
00092	Send broadcast	command	com/adobe/air/AndroidActivityWrapper.java
00036	Get resource file from res/raw directory	reflection	c/m/x/a/ep/ax.java com/adobe/air/AndroidActivityWrapper.java com/adobe/air/ResourceFileManager.java com/distriqt/extension/nativewebview/controller/browser/BrowserView.java
00064	Monitor incoming call status	control	com/adobe/air/telephony/AndroidTelephonyManager.java

RULE ID	BEHAVIOUR	LABEL	FILES
00051	Implicit intent(view a web page, make a phone call, etc.) via setData	control	c/m/x/a/ep/ax.java com/distriqt/extension/nativewebview/controller/webview/AdvancedWebView.java
00062	Query WiFi information and WiFi Mac Address	wifi collection	com/adobe/air/net/AndroidNetworkInfo.java com/adobe/air/wand/connection/WandWebSocket.java
00116	Get the current WiFi MAC address and put it into JSON	wifi collection	com/adobe/air/wand/connection/WandWebSocket.java
00076	Get the current WiFi information and put it into JSON	collection wifi	com/adobe/air/wand/connection/WandWebSocket.java
00023	Start another application from current application	reflection control	com/distriqt/extension/nativewebview/controller/browser/BrowserView.java
00009	Put data in cursor to JSON object	file	com/distriqt/extension/nativewebview/controller/NativeWebView.java
00106	Get the currently formatted WiFi IP address	collection wifi	com/adobe/air/net/AndroidNetworkInfo.java
00130	Get the current WIFI information	wifi collection	c/m/x/a/ep/aw.java com/adobe/air/net/AndroidNetworkInfo.java
00134	Get the current WiFi IP address	wifi collection	com/adobe/air/net/AndroidNetworkInfo.java
00082	Get the current WiFi MAC address	collection wifi	com/adobe/air/net/AndroidNetworkInfo.java
00075	Get location of the device	collection location	com/adobe/air/AndroidGcmRegistrationService.java com/adobe/air/location/Geolocation.java

RULE ID	BEHAVIOUR	LABEL	FILES
00091	Retrieve data from broadcast	collection	com/adobe/air/AndroidGcmIntentService.java com/adobe/air/RemoteDebuggerListenerDialog.java
00123	Save the response to JSON after connecting to the remote server	network command	com/adobe/air/AndroidGcmIntentService.java
00089	Connect to a URL and receive input stream from the server	command network	com/adobe/air/AndroidGcmIntentService.java com/distriqt/extension/nativewebview/controller/tasks/NativeWebViewLoadTask.java
00030	Connect to the remote server through the given URL	network	com/adobe/air/AndroidGcmIntentService.java com/distriqt/extension/nativewebview/controller/tasks/NativeWebViewLoadTask.java
00077	Read sensitive data(SMS, CALLLOG, etc)	collection sms calllog calendar	com/distriqt/extension/nativewebview/utils/ContentProviderUtils.java
00031	Check the list of currently running applications	reflection collection	com/adobe/air/ShakeListenerService.java
00056	Modify voice volume	control	com/distriqt/extension/volume/controller/VolumeController.java
00109	Connect to a URL and get the response code	network command	com/distriqt/extension/nativewebview/controller/tasks/NativeWebViewLoadTask.java
00137	Get last known location of the device	location collection	com/adobe/air/AndroidGcmRegistrationService.java
00115	Get last known location of the device	collection location	com/adobe/air/AndroidGcmRegistrationService.java
00113	Get location and put it into JSON	collection location	com/adobe/air/AndroidGcmRegistrationService.java

RULE ID	BEHAVIOUR	LABEL	FILES
00016	Get location info of the device and put it to JSON object	location collection	com/adobe/air/AndroidGcmRegistrationService.java
00183	Get current camera parameters and change the setting.	camera	com/adobe/air/AndroidCamera.java
00012	Read data and put it into a buffer stream	file	com/adobe/air/ApplicationFileManager.java
00033	Query the IMEI number	collection	c/m/x/a/ep/aw.java

ABUSED PERMISSIONS

TYPE	MATCHES	PERMISSIONS
Malware Permissions	10/25	android.permission.READ_PHONE_STATE, android.permission.GET_ACCOUNTS, android.permission.GET_TASKS, android.permission.WAKE_LOCK, android.permission.VIBRATE, android.permission.CAMERA, android.permission.INTERNET, android.permission.WRITE_EXTERNAL_STORAGE, android.permission.ACCESS_NETWORK_STATE, android.permission.ACCESS_WIFI_STATE
Other Common Permissions	1/44	com.google.android.c2dm.permission.RECEIVE

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
distriqt.com	ok	**IP:** 173.236.207.222 **Country:** United States of America **Region:** California **City:** Brea **Latitude:** 33.930222 **Longitude:** -117.888420 **View:** Google Map
www.openssl.org	ok	**IP:** 34.49.79.89 **Country:** United States of America **Region:** Texas **City:** Houston **Latitude:** 29.941401 **Longitude:** -95.344498 **View:** Google Map
s3-us-west-1.amazonaws.com	ok	**IP:** 52.219.193.32 **Country:** United States of America **Region:** Washington **City:** Seattle **Latitude:** 47.627499 **Longitude:** -122.346199 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
dh8vjmvwgc27o.cloudfront.net	ok	No Geolocation information available.
gamespace.adobe.com	ok	No Geolocation information available.
www.adobe.com	ok	**IP:** 2.21.20.145 **Country:** Spain **Region:** Madrid, Comunidad de **City:** Madrid **Latitude:** 40.416500 **Longitude:** -3.702560 **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
www.macromedia.com	ok	**IP:** 184.25.50.83 **Country:** United States of America **Region:** Florida **City:** Tampa **Latitude:** 27.947519 **Longitude:** -82.458427 **View:** Google Map
airdownload2.adobe.com	ok	**IP:** 69.192.160.136 **Country:** United States of America **Region:** Florida **City:** Fort Lauderdale **Latitude:** 26.122311 **Longitude:** -80.143379 **View:** Google Map

DOMAIN	STATUS	GEOLOCATION
www.amazon.com	ok	**IP:** 13.32.143.59 **Country:** Finland **Region:** Uusimaa **City:** Helsinki **Latitude:** 60.169521 **Longitude:** 24.935450 **View:** Google Map
ns.adobe.com	ok	No Geolocation information available.
dashif.org	ok	**IP:** 185.199.109.153 **Country:** United States of America **Region:** Pennsylvania **City:** California **Latitude:** 40.065632 **Longitude:** -79.891708 **View:** Google Map

EMAILS

EMAIL	FILE
ftp@example.com	apktool_out/lib/armeabi-v7a/libCore.so
ftp@example.com	lib/armeabi-v7a/libCore.so

TRACKERS

TRACKER	CATEGORIES	URL
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

🔑 HARDCODED SECRETS

POSSIBLE SECRETS
"use_fingerprint_to_authenticate_key" : "use_fingerprint_to_authenticate_key"
"districqt_password" : "Password"
"password" : "Password"
b3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef
SQmHWbTAzPlYuz5I3xZRZNLM/2+IGX009ow9MnjYfrI=
tSH6JN0/dsR0FAYjQVtAYWAamOw3jEQmk6Hr8jJN+yrtPJ4ZwRFL84dAlVlDBCND
hp8obFMJgqHXmaR5pMrBIn7HvqDUI8ERyuIbnl0iT/M=
G68A6YJ+VRJhgHK56Kx1RoGHOyqehPG7tlyyPwtcr7Q=
ntbFRCAexgxz9p8O68TxIQjW9W7nZKRNbG91vq8F9ro=
QIWClwyA1htDcymLB9H+9tV5qeIhlSOa2TsbKDGB4CU=
AIzaSyDRKQ9d6kfsoZT2lUnZcZnBYvH69HExNPE

POSSIBLE SECRETS
3940200619639447921227904010014361380507973927046544666794690527962765939911326356939895630815229491355443365394264 3
kiOoUcTqb+PvEdOeeDwNvvUZgbOHeCWSZHc9NNTPPv4=
6864797660130609714981900799081393217269435300143305409394463459185543183397655394245057746333217197532963996371363321113864768612440380340372808892707005449
OU2zTkMb3xVWxjElhSJNJtcyjBcBIax5KghmsB2DrHu3HRhgp4Bz1cQIIaak8Abf
1157920892103562487626974469494075735299969552241357603424222590610685120443 69
B3EEABB8EE11C2BE770B684D95219ECB
0aMkajKGfxJjxUakLLOcj8JypKv0GmCb3d+C/AP1yzc=
5Un4Bxdp8gVIANCZ39+qNPpJwSMKWP26YPuxiQ9CnPTd/FlU4AIzDaH9PI9I+CrN
JpT53kCFZ5UGhS3QgNfIxU7Zo+2b3P+3vnYveTkMBHt4zfnotqnDwQTaAD1ryBW9
55W269KXvkwdzl5sfb0CcKPmBnPIftmJMRWEHFEIHMVBNbB9RYoQD/JeAhpTyftv
zAquriPjpzqGJfvs/9ulqqLxOML+UEqSlyjOz6Tu5VU=
teIp99oid1pENGWnU++9yOPCIwtIDIwejcakl+LfK5qHHKbt0MJt+8BqbhD17b1n
m2+gcfdQWoY+6hOETk2mr0SsbjGMFJBzTmSItOYkEfM=
3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f
NREPPB/9iy6pGr9Pw6YHALTcoiK6Qv0Fu8JVtmSXvzQ=
3940200619639447921227904010014361380507973927046544666794829340424572177149687032904726608825893800186161606973112319

POSSIBLE SECRETS
diFehzLUdSyhsDAHjo1jRWbuUSlDLM7ewQWDc6EGa5SkktywcOnUZVN2l852D8v/
Ye7G7hL63+8nOBoyCAHdjfK62rvCOKz3+aC1KA/K9CI=
5ac635d8aa3a93e7b3ebbd55769886bc651d06b0cc53b0f63bce3c3e27d2604b
xRFu2EA0XhZqR4z5v1+z5DRPRDh4cLaTVyZWq8w+32M=
DjhY2o1Svq1HpINv7cU+bAqV+OA81bMZ6vkVBk0u3II=
c760NRjk4Ctk2HA0ROzb7VHBeyDIvOdXhTBmaaREC+Y=
qDz6YvDkhwdxUOtNXedEKNdh2XDWXqUECYckxUUtMRo=
4Df+wFSysP9SafTWPUlnClwqa+KS42poxSq2xHfYKTY=
Vz6KZKN/XNSe7DawDVk5XNlgz1HLOOLd+9M1b4lusVA=
DdZDLurYd8cqlTxFH9iUg4PWLqXdMHMkdrTyCVNVmPtO8AJJSQ+/YGXoMqGNOXWI
115792089210356248762697446949407573530086143415290314195533631308867097853951
9a04f079-9840-4286-ab92-e65be0885f95
051953eb9618e1c9a1f929a21a0b68540eea2da725b99b315f3b8b489918ef109e156193951ec7e937b1652c0bd3bb1bf073573df883d2c34f1ef451fd46b503f00
BDp2p9FkJRWhLjM5/HGlBtfI2hTpjdS5yJQGMqe31LtNjFTgL+0QOyyChfmPPFl0
1lkHdmwdwv9wD8tmJQC+h66q1PQxvS+V9UrDno8I9cxHFnF0E43buTrJO+G+/gQl
phpjyfBMe8u7C5auGMsy22WXoT6iMDb5qqttOP4sXOBlc73QdE1wdYLJ++PsHndY

POSSIBLE SECRETS
M1NS9rNHdzevdCO1BkBQDrEtWalzliBN1oXlHuD/PStxAuVrokFwJ8FTE8R3woq0
dUZXsTQGXogdq7xqgYL8i0iimZLTpa9AoXZpRO79MP7o6nVl+DoNjuCg63H0zXDK
LOklmrwaQ0v3CGeP+ZosklY8SbmufmvNG6auvqsL+bGnLcr54FaTv3bt+awlDR0E
c6858e06b70404e9cd9e3ecb662395b4429c648139053fb521f828af606b4d3dbaa14b5e77efe75928fe1dc127a2ffa8de3348b3c1856a429bf97e7e31c2e5bd66
DPtJycwRqj/e0TdTHULzeUhZhWJ1IU3iwhH90sUbn4eYKEdB5HI7UC0PtJgg2RSN
7ZWY64KY7J2YIO2MjOydvOydhCDshKDtg50=
gccLIpNanlTav8umvHfA6CkZesdxV9Cr39ehhj7Z8L8=
4fe342e2fe1a7f9b8ee7eb4a7c0f9e162bce33576b315ececbb6406837bf51f5
11839296a789a3bc0045c8a5fb42c7d1bd998f54449579b446817afbd17273e662c97ee72995ef42640c550b9013fad0761353c7086a272c24088be94769fd16650
6864797660130609714981900799081393217269435300143305409394463459185543183397656052122559640661454554977296311391480858037121987999716643812574028291115057151
got2az0DwXyMWaLpfVutWfEF1l3X50FJhmqzREDcTA8=
6b17d1f2e12c4247f8bce6e563a440f277037d812deb33a0f4a13945d898c296
2KfbjNqpINmB2KfYptmElNmF24zauiDYs9uSINin2YbYqtiu2KfYqCDaqdix24zaug==
HW6DUu9hdQUUJG4hyzA4/jDFe17EFpXdJQ2aqCpScU07e6PXExB1P1rW0uW0StIw
4Nk49DU1yHD/oE1MfAOMbRwhDipAhidA7tdJouMJQrI=
TxRdKOZ0pZeBXpIwiLITX81ZqIx50eBVN3DINE4ZBUPdk4novnMzQn3dOLT7/176

POSSIBLE SECRETS
aa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f25dbf55296c3a545e3872760ab7
XCJaUXNSa18os9LIeCcjZdYTv1kZvdxKgQEEsV6JTUc=
0000016742C00BDA259000000168CE0F13200000016588840DCE7118A0002FBF1C31C3275D78
2LHYpyDYp9mG2KrYrtin2Kgg2qnZhtuM2K8g24zaqSDZgdin24zZhA==
A9jthiAQc+izVBr4mJNKEZTv7NXyHy0tI8Qg667eCzo=
9KTvYPBd7MH2ciAlBu9OHvde4n0Fwv5nDeizahStujRhSUn5FAOJjVUu69hMaCIH

PLAYSTORE INFORMATION

Title: nomo - Sobriety Clocks

Score: 4.12 **Installs:** 50,000+ **Price:** 0 **Android Version Support:** **Category:** Lifestyle **Play Store URL:** air.com.parkerstech.day

Developer Details: Parker Stech, Parker+Stech, None, https://saynomo.com, parker@saynomo.com,

Release Date: Nov 8, 2016 **Privacy Policy:** Privacy link

Description:

Hi! My name is Parker. I'm not a company. I'm just a guy in recovery who made Nomo as a tool to keep me on track and motivated. Nomo is short for, "No More". It's a passion project of mine and I hope it helps you as much as it has been helping me! If you're looking for a simple clock that can track the number of days you've been sober/clean/etc, then Nomo is perfect for you. You can create as many clocks as you need for any hurts, habits, or hang ups. Your clocks are completely private by default and will count those days for you. If you're looking for something more, just check under the hood. Nomo has tons of optional features like an encouragement wall from the community, accountability partner searching, clock sharing, private messaging with partners, milestone awards, journaling, little games/exercises to help you refocus when you're tempted, and tons more! What makes Nomo so great? • Create as many sobriety clocks as you need • Find accountability parters! • Share selected clocks with accountability partners • Send a notification to partners when you're feeling tempted • Send/Receive notifications when a clock has been reset • Get a detailed breakdown of your progress down to the minute • See how much money you've saved by not supporting your habit • Earn chips when you reach certain milestones in your recovery • Submit and read encouragements from the community • View all of your chips at once to keep you encouraged • Tap the “check in” button on your shared clocks to show accountability partners that you’re active in your sobriety • Mini-distraction exercises to help you refocus when you’re feeling tempted • Prevent someone from accessing your Nomo app with a secure PIN and/or Biometrics. Nomo is perfect for anyone recovering from any kind of hurt, habit, or hangup. I hope it’s a valuable tool for you in your recovery.

SCAN LOGS

Timestamp	Event	Error
2024-11-23 20:01:41	Generating Hashes	OK
2024-11-23 20:01:41	Extracting APK	OK
2024-11-23 20:01:41	Unzipping	OK
2024-11-23 20:01:42	Getting Hardcoded Certificates/Keystores	OK
2024-11-23 20:01:42	Parsing APK with androguard	OK
2024-11-23 20:01:47	Parsing AndroidManifest.xml	OK
2024-11-23 20:01:47	Extracting Manifest Data	OK
2024-11-23 20:01:47	Manifest Analysis Started	OK
2024-11-23 20:01:47	Performing Static Analysis on: nomo (air.com.parkerstech.day)	OK

2024-11-23 20:01:47	Fetching Details from Play Store: air.com.parkerstech.day	OK
2024-11-23 20:01:48	Checking for Malware Permissions	OK
2024-11-23 20:01:48	Fetching icon path	OK
2024-11-23 20:01:48	Library Binary Analysis Started	OK
2024-11-23 20:01:48	Analyzing apktool_out/lib/armeabi-v7a/libysshared.so	OK
2024-11-23 20:01:48	Analyzing apktool_out/lib/armeabi-v7a/libCore.so	OK
2024-11-23 20:01:49	Analyzing apktool_out/lib/armeabi-v7a/libc++_shared.so	OK
2024-11-23 20:01:49	Analyzing lib/armeabi-v7a/libysshared.so	OK
2024-11-23 20:01:49	Analyzing lib/armeabi-v7a/libCore.so	OK
2024-11-23 20:01:50	Analyzing lib/armeabi-v7a/libc++_shared.so	OK
2024-11-23 20:01:50	Reading Code Signing Certificate	OK

2024-11-23 20:01:51	Running APKiD 2.1.5	OK
2024-11-23 20:01:56	Detecting Trackers	OK
2024-11-23 20:01:58	Decompiling APK to Java with JADX	OK
2024-11-23 20:02:29	Converting DEX to Smali	OK
2024-11-23 20:02:29	Code Analysis Started on - java_source	OK
2024-11-23 20:02:33	Android SAST Completed	OK
2024-11-23 20:02:33	Android API Analysis Started	OK
2024-11-23 20:03:06	Android API Analysis Completed	OK
2024-11-23 20:03:07	Android Permission Mapping Started	OK
2024-11-23 20:03:09	Android Permission Mapping Completed	OK
2024-11-23 20:03:10	Android Behaviour Analysis Started	OK

2024-11-23 20:03:12	Android Behaviour Analysis Completed	OK
2024-11-23 20:03:12	Extracting Emails and URLs from Source Code	OK
2024-11-23 20:03:12	Email and URL Extraction Completed	OK
2024-11-23 20:03:12	Extracting String data from APK	OK
2024-11-23 20:03:13	Extracting String data from SO	OK
2024-11-23 20:03:13	Extracting String data from Code	OK
2024-11-23 20:03:13	Extracting String values and entropies from Code	OK
2024-11-23 20:03:14	Performing Malware check on extracted domains	OK
2024-11-23 20:03:16	Saving to Database	OK

Report Generated by - MobSF v4.2.4

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.