STATE UNIVERSITY OF NEW YORK AT BINGHAMTON

CS 527 MOBILE SYSTE SECURITY

PROJECT 2

MALWARE ANALYSIS

VENKATNARAYAN GNANAGURUPARAN

B01013037

CONTENTS

BENIGN APPLICATONS

BENIGN APP 1 – BIRMINGHAMMAIL

In this report, we conduct an analysis of the BirminghamMail newspaper app using both static and dynamic malware analysis techniques. The objective is to understand the behavior of the app, identify any malicious activities, and draw conclusions based on the analysis performed.

The Birmingham Mail is an Android application for tabloid newspaper based in Birmingham.

STATIC ANALYSIS - ANDROWARN

The Androwarn report for the "Birmingham local news" application version 2.3, with package name com.birmingham.free.news, reveals potential telephony identifiers leakage issues. These include accessing sensitive telephony-related data such as SIM provider country code, current registered operator's MCC, MCC+MNC of the SIM provider, device phone type value, numeric name of the current registered operator, and radio technology currently in use. The risks associated with these actions vary from medium to low, posing potential privacy concerns and security risks. Recommendations include reviewing the necessity of accessing telephony data, implementing proper permission handling, data minimization strategies, encryption for sensitive data, and conducting a thorough security review to identify and address any additional vulnerabilities. These measures are crucial for enhancing the privacy and security of the application and ensuring compliance with relevant regulations.

```
32        "analysis_results": [
33            [
34                "telephony_identifiers_leakage",
35                [
36                    "This application reads the ISO country code equivalent for the SIM provider's country code",
37                    "This application reads the ISO country code equivalent of the current registered operator's MCC (Mobile
  Country Code)",
38                    "This application reads the MCC+MNC of the provider of the SIM",
39                    "This application reads the device phone type value",
40                    "This application reads the numeric name (MCC+MNC) of current registered operator",
41                    "This application reads the radio technology (network type) currently in use on the device for data
  transmission"
42                ]
43            ],
```

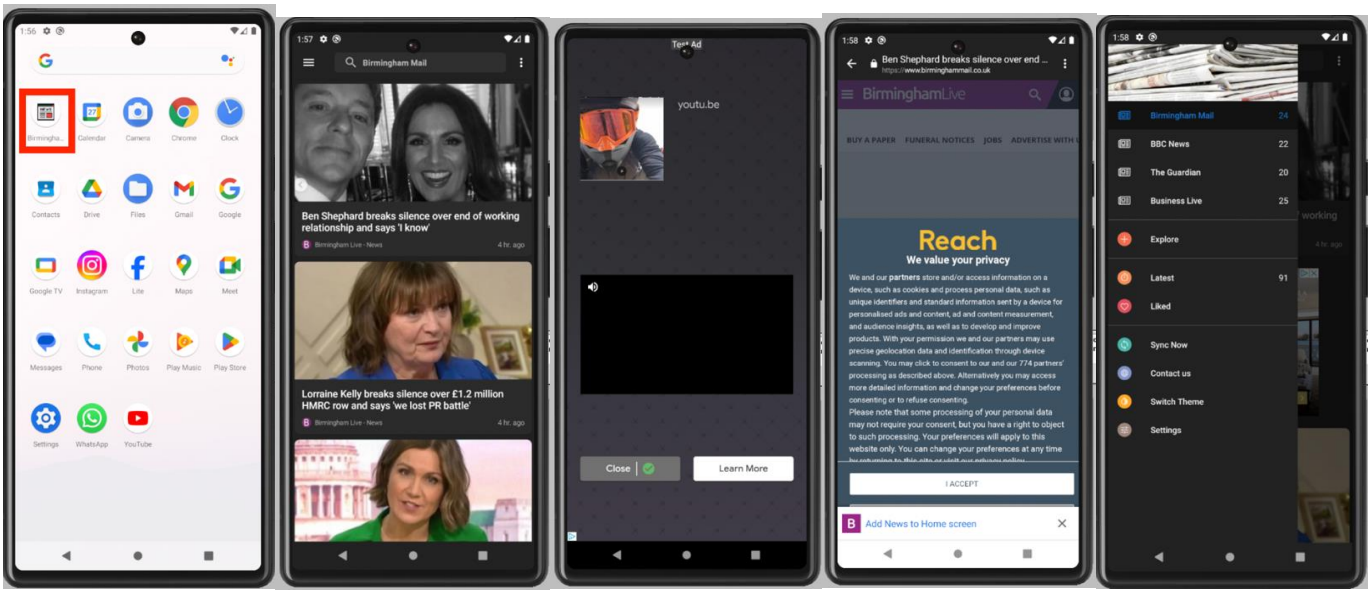
```
                "telephony_services_abuse",
                [
                    "This application makes phone calls"
                ]
            ],
            [
                "audio_video_eavesdropping",
                []
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address ' returned no addresses for  ; port
is out of range' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address '' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/net/Proxy;-
>type()Ljava/net/Proxy$Type;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'timeout' on the 'N/A' port "
                ]
            ],
            [
                "PIM_data_leakage",
                [
                    "This application accesses the downloads folder",
                    "This application accesses data stored in the clipboard"
                ]
            ],
            [
                "code_execution",
                [
                    "This application loads a native library"
                ]
            ]
        ]
    },
```

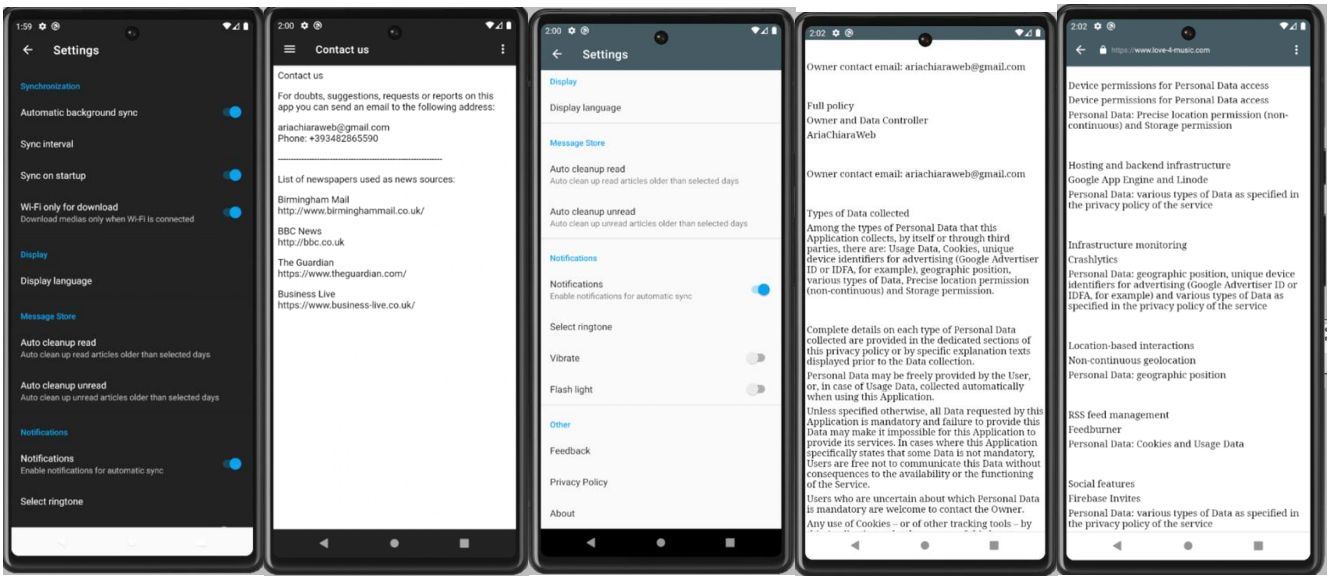

There are potential telephony services abuse through unauthorized phone calls, posing a high risk to users' privacy and potentially leading to financial costs. Additionally, the application opens suspicious connections to remote addresses, which could indicate malicious behavior or vulnerabilities. Furthermore, there's access to PIM data such as the downloads folder and clipboard, raising concerns about data leakage. Moreover, the application loads a native library, suggesting potential code execution vulnerabilities. While no instances of audio/video eavesdropping were found, continuous monitoring of these functionalities is essential. Recommendations include implementing proper permission handling, user consent mechanisms, and thorough security reviews to address these vulnerabilities and enhance the application's privacy and security.

```
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.FLASHLIGHT',\n 'android.permission.FOREGROUND_SERVICE',\n 'android.permission.INTERNET',\n
'android.permission.POST_NOTIFICATIONS',\n 'android.permission.READ_EXTERNAL_STORAGE',\n
'android.permission.RECEIVE_BOOT_COMPLETED',\n 'android.permission.VIBRATE',\n 'android.permission.WAKE_LOCK',\n
'android.permission.WRITE_EXTERNAL_STORAGE',\n 'com.google.android.c2dm.permission.RECEIVE',\n
'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE',\n 'com.google.android.gms.permission.AD_ID',\n
'com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY']",
                    "Implied: []",
                    "Declared: []"
                ]
            ],
            [
                "features",
                [
                    "android.hardware.location.network",
                    "android.hardware.touchscreen",
                    "android.hardware.wifi"
                ]
            ],
            [
                "libraries",
                [
                    "androidx.window.extensions",
                    "androidx.window.sidecar"
                ]
            ]
        ]
    },
```


the permissions requested suggest that the application requires access to network connectivity, storage, notifications, and other device features. The declared features indicate reliance on location services, touchscreen functionality, and Wi-Fi capabilities. Additionally, the use of specific libraries, such as androidx.window.extensions and androidx.window.sidecar, may imply UI or window management functionalities. It's essential to ensure that these permissions and features are necessary for the application's functionality and that proper security measures are in place to protect user data and privacy.

APP SCREENSHOTS



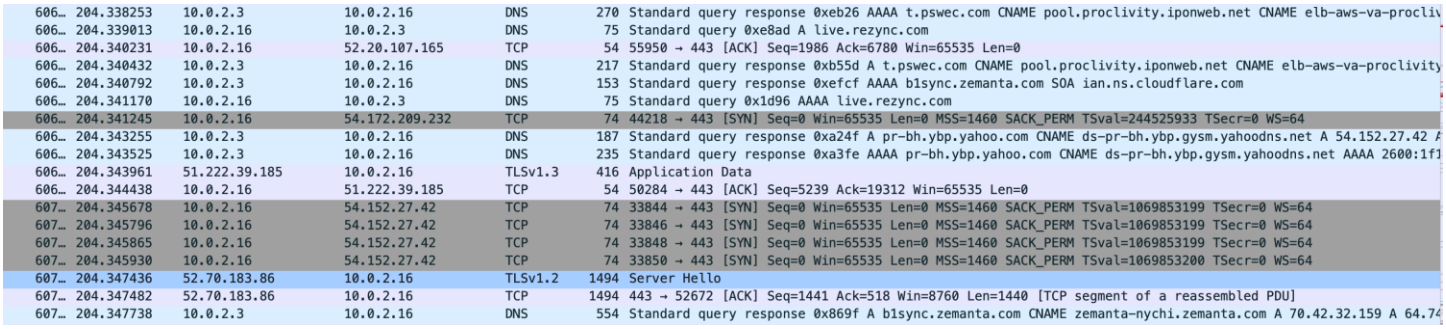


DYNAMIC ANALYSIS - WIRESHARK

Total Number of Packets Traced: 68872 Packets

DNS Packets : 1693 Packets

DHCP Packets : 8 Packets



606…	204.338253	10.0.2.3	10.0.2.16	DNS	270	Standard query response 0xeb26 AAAA t.pswec.com CNAME pool.proclivity.iponweb.net CNAME elb-aws-va-procliv
606…	204.339013	10.0.2.16	10.0.2.3	DNS	75	Standard query 0xe8ad A live.rezync.com
606…	204.340231	10.0.2.16	52.20.107.165	TCP	54	55950 → 443 [ACK] Seq=1986 Ack=6780 Win=65535 Len=0
606…	204.340432	10.0.2.3	10.0.2.16	DNS	217	Standard query response 0xb55d A t.pswec.com CNAME pool.proclivity.iponweb.net CNAME elb-aws-va-proclivity
606…	204.340792	10.0.2.3	10.0.2.16	DNS	153	Standard query response 0xefcf AAAA b1sync.zemanta.com SOA ian.ns.cloudflare.com
606…	204.341170	10.0.2.16	10.0.2.3	DNS	75	Standard query 0x1d96 AAAA live.rezync.com
606…	204.341245	10.0.2.16	54.172.209.232	TCP	74	44218 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=244525933 TSecr=0 WS=64
606…	204.343255	10.0.2.3	10.0.2.16	DNS	187	Standard query response 0xa24f A pr-bh.ybp.yahoo.com CNAME ds-pr-bh.ybp.gysm.yahoodns.net A 54.152.27.42 A
606…	204.343525	10.0.2.3	10.0.2.16	DNS	235	Standard query response 0xa3fe AAAA pr-bh.ybp.yahoo.com CNAME ds-pr-bh.ybp.gysm.yahoodns.net AAAA 2600:1f1
606…	204.343961	51.222.39.185	10.0.2.16	TLSv1.3	416	Application Data
606…	204.344438	10.0.2.16	51.222.39.185	TCP	54	50284 → 443 [ACK] Seq=5239 Ack=19312 Win=65535 Len=0
607…	204.345678	10.0.2.16	54.152.27.42	TCP	74	33844 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1069853199 TSecr=0 WS=64
607…	204.345796	10.0.2.16	54.152.27.42	TCP	74	33846 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1069853199 TSecr=0 WS=64
607…	204.345865	10.0.2.16	54.152.27.42	TCP	74	33848 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1069853199 TSecr=0 WS=64
607…	204.345930	10.0.2.16	54.152.27.42	TCP	74	33850 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=1069853200 TSecr=0 WS=64
607…	204.347436	52.70.183.86	10.0.2.16	TLSv1.2	1494	Server Hello
607…	204.347482	52.70.183.86	10.0.2.16	TCP	1494	443 → 52672 [ACK] Seq=1441 Ack=518 Win=8760 Len=1440 [TCP segment of a reassembled PDU]
607…	204.347738	10.0.2.3	10.0.2.16	DNS	554	Standard query response 0x869f A b1sync.zemanta.com CNAME zemanta-nychi.zemanta.com A 70.42.32.159 A 64.74

The application actively initiates DNS queries targeting blog websites to retrieve and share news articles. This behavior indicates that the app is designed to fetch and distribute information from online sources, potentially for the purpose of providing news updates to users. However, further analysis is required to determine the specific nature of the articles being accessed and the manner in which they are shared within the application. Additionally, monitoring DNS activity can help in assessing the scope and frequency of these queries, providing insights into the app's news-fetching capabilities and its impact on device performance and user privacy.

CONCLUSION

The application serves as a news aggregator, offering users a platform to access diverse news articles and information. Through DNS queries, it retrieves data from associated links, enabling users to explore a range of news sources and articles seamlessly. This functionality ensures users stay informed with up-to-date news content and facilitates easy access to relevant information.

Moreover, the application is considered benign, as it does not pose any risks to user devices, data, or privacy. It operates within expected parameters, fulfilling its intended purpose without engaging in any malicious behavior. Users can confidently interact with the application, assured of its safety and reliability, without worrying about potential harm or security threats.

BENIGN APP 2 – XLAUNCHER

Xlauncher app acts as the gateway to the user's Android device, replacing the default home screen with a customizable interface tailored to individual preferences. Through features like theme selection, wallpaper customization, and icon pack options, users can personalize the appearance of their device's home screen. Additionally, launcher apps often offer tools for organizing installed applications, streamlining navigation through intuitive gesture controls, and optimizing device performance for smoother operation. With the ability to enhance privacy and security through features like app locking and permission controls, a launcher app serves as a central hub for users to interact with their devices efficiently and seamlessly.

STATIC ANALYSIS - ANDROWARN


```
        "analysis_results": [
            [
                "telephony_identifiers_leakage",
                [
                    "This application reads the ISO country code equivalent for the SIM provider's country code",
                    "This application reads the ISO country code equivalent of the current registered operator's MCC (Mobile Country Code)",
                    "This application reads the MCC+MNC of the provider of the SIM",
                    "This application reads the SIM's serial number",
                    "This application reads the Service Provider Name (SPN)",
                    "This application reads the constant indicating the state of the device SIM card",
                    "This application reads the current data connection state",
                    "This application reads the current location of the device",
                    "This application reads the device phone type value",
                    "This application reads the neighboring cell information of the device",
                    "This application reads the numeric name (MCC+MNC) of current registered operator",
                    "This application reads the operator name",
                    "This application reads the radio technology (network type) currently in use on the device for data transmission",
                    "This application reads the unique device ID, i.e the IMEI for GSM and the MEID or ESN for CDMA phones",
                    "This application reads the unique subscriber ID, for example, the IMSI for a GSM phone",
                    "This application reads the Cell ID value",
                    "This application reads the Location Area Code value"
                ]
            ],
```


Telephony Identifiers Leakage:

The application under analysis exhibits concerning behavior regarding the access and retrieval of telephony-related identifiers. These include:

- Reading ISO country codes for SIM provider and registered operator.
- Accessing MCC+MNC of the SIM provider and the SIM's serial number.
- Retrieving Service Provider Name (SPN) and device SIM card state.
- Obtaining current data connection state, device location, phone type, and neighboring cell information.
- Accessing numeric name (MCC+MNC) and operator name of the current registered operator.
- Reading radio technology for data transmission, unique device ID (IMEI/MEID/ESN), and unique subscriber ID (IMSI).
- Retrieving Cell ID and Location Area Code values.

```
                "permissions",
                [
                    "Asked: ['android.hardware.camera',\n 'android.hardware.camera.autofocus',\n
'android.hardware.camera.flash',\n 'android.permission.ACCESS_COARSE_LOCATION',\n 'android.permission.ACCESS_FINE_LOCATION',\n
'android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_NOTIFICATION_POLICY',\n
'android.permission.ACCESS_WEATHERCLOCK_PROVIDER',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.BIND_APPWIDGET',\n 'android.permission.BLUETOOTH',\n 'android.permission.BLUETOOTH_ADMIN',\n
'android.permission.BLUETOOTH_CONNECT',\n 'android.permission.BROADCAST_STICKY',\n 'android.permission.CAMERA',\n
'android.permission.CHANGE_NETWORK_STATE',\n 'android.permission.CHANGE_WIFI_STATE',\n
'android.permission.EXPAND_STATUS_BAR',\n 'android.permission.FLASHLIGHT',\n 'android.permission.FOREGROUND_SERVICE',\n
'android.permission.INTERNET',\n 'android.permission.MODIFY_AUDIO_SETTINGS',\n 'android.permission.POST_NOTIFICATIONS',\n
'android.permission.QUERY_ALL_PACKAGES',\n 'android.permission.READ_EXTERNAL_STORAGE',\n
'android.permission.READ_PHONE_STATE',\n 'android.permission.READ_SETTINGS',\n 'android.permission.READ_SYNC_SETTINGS',\n
'android.permission.RECEIVE_USER_PRESENT',\n 'android.permission.REQUEST_DELETE_PACKAGES',\n
'android.permission.SET_WALLPAPER',\n 'android.permission.SET_WALLPAPER_HINTS',\n 'android.permission.SYSTEM_ALERT_WINDOW',\n
'android.permission.VIBRATE',\n 'android.permission.WAKE_LOCK',\n 'android.permission.WRITE_EXTERNAL_STORAGE',\n
'android.permission.WRITE_SETTINGS',\n 'android.permission.WRITE_SYNC_SETTINGS',\n
'com.android.ContactWidget.permission.WRITE_SETTINGS',\n 'com.android.alarm.permission.SET_ALARM',\n
'com.android.launcher.permission.INSTALL_SHORTCUT',\n 'com.android.launcher.permission.READ_SETTINGS',\n
'com.android.launcher.permission.WRITE_SETTINGS',\n 'com.android.launcher3.permission.READ_SETTINGS',\n
'com.android.launcher3.permission.WRITE_SETTINGS',\n 'com.google.android.gms.permission.AD_ID',\n
'com.huawei.android.totemweather.permission.ACCESS_WEATHERCLOCK_PROVIDER',\n
'huawei.android.permission.HW_SIGNATURE_OR_SYSTEM']",
                    "Implied: []",
                    "Declared: ['com.ioslauncher.free2.permission.READ_SETTINGS',\n
'com.ioslauncher.free2.permission.WRITE_SETTINGS']"
                ]
            ],
            [
                "features",
                [
                    "android.hardware.bluetooth",
                    "android.hardware.camera",
                    "android.hardware.camera.autofocus",
                    "android.hardware.LOCATION",
                    "android.hardware.location.GPS"
                ]
            ],
            [
                "libraries",
                [
                    "org.apache.http.legacy"
                ]
            ]
```


The application requests a comprehensive set of permissions, including access to device hardware and various system functionalities. Key permissions include camera access, location services (coarse and fine), network state, Bluetooth, camera control, flashlight, internet access, audio settings modification, storage access, and system settings manipulation. Additionally, there are permissions related to widget binding, wallpaper setting, system alerts, and launcher configuration. It is noteworthy that the application declares specific permissions for reading and writing settings in the launcher and contaect widget contexts.

The application utilizes several hardware features, including Bluetooth and camera capabilities such as autofocus. Location-related features are also employed, including GPS functionality. These features indicate the application's reliance on device hardware for various functionalities, including communication, multimedia, and location-based services.

The application utilizes the "org.apache.http.legacy" library, which suggests the use of Apache HTTP components for networking tasks. While this library is commonly used for HTTP communication, its usage may pose security risks if not properly maintained due to potential vulnerabilities or deprecated features.

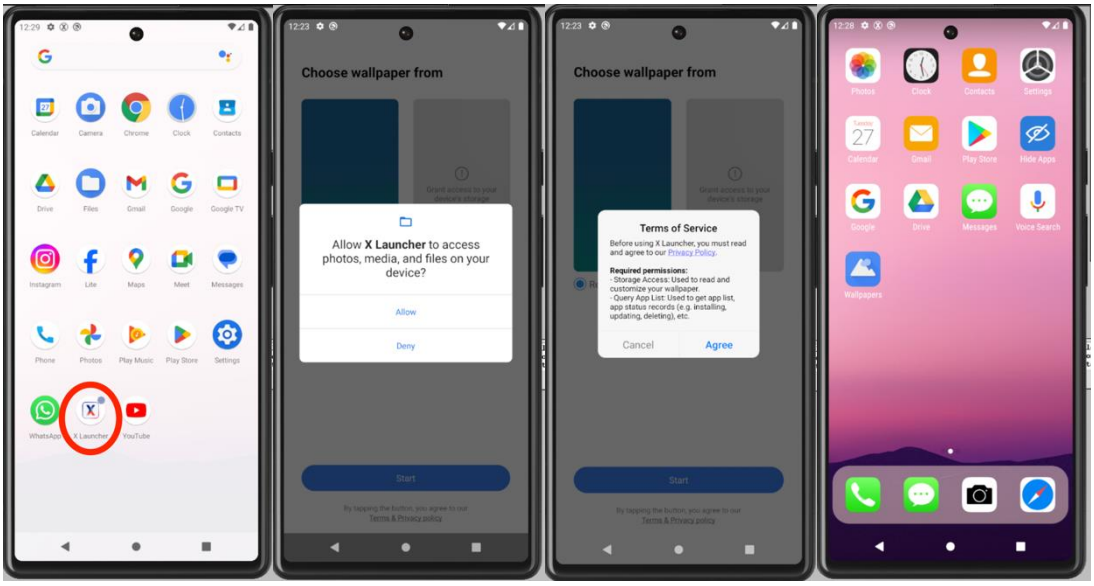
DYNAMIC ANALYSIS – WIRESHARK

Total number of packets – 20176
Number of DNS Packets – 748
Number of TCP Packets - 10872

2835	43.456518	10.0.2.16	10.0.2.3	DNS	80	Standard query 0x4c46 AAAA beacons.gcp.gvt2.com
2836	43.460376	142.250.64.110	10.0.2.16	QUIC	66	Protected Payload (KP0)
2837	43.487538	10.0.2.16	10.0.2.3	DNS	97	Standard query 0x18f1 AAAA mobileconfiguration-pa.googleapis.com
2838	43.490754	10.0.2.3	10.0.2.16	DNS	138	Standard query response 0x4c46 AAAA beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com AAAA 2607:f8b0
2839	43.491327	10.0.2.16	10.0.2.3	DNS	80	Standard query 0x5e10 A beacons.gcp.gvt2.com
2840	43.491961	10.0.2.3	10.0.2.16	DNS	126	Standard query response 0x5e10 A beacons.gcp.gvt2.com CNAME beacons-handoff.gcp.gvt2.com A 142.250.64.99
2841	43.502071	10.0.2.3	10.0.2.16	DNS	209	Standard query response 0x18f1 AAAA mobileconfiguration-pa.googleapis.com AAAA 2607:f8b0:4006:820::200a AA
2842	43.502397	10.0.2.16	10.0.2.3	DNS	97	Standard query 0x8815 A mobileconfiguration-pa.googleapis.com
2843	43.514823	10.0.2.3	10.0.2.16	DNS	353	Standard query response 0x8815 A mobileconfiguration-pa.googleapis.com A 142.251.32.106 A 142.250.65.234 A
6699	62.823750	10.0.2.16	10.0.2.3	DNS	71	Standard query 0x4764 AAAA i.ytimg.com
6700	62.824006	10.0.2.16	10.0.2.3	DNS	71	Standard query 0xfe1a A i.ytimg.com
6701	62.836283	10.0.2.3	10.0.2.16	DNS	327	Standard query response 0xfe1a A i.ytimg.com A 142.251.40.246 A 172.217.165.150 A 142.250.81.246 A 142.250
6702	62.836410	10.0.2.3	10.0.2.16	DNS	183	Standard query response 0x4764 AAAA i.ytimg.com AAAA 2607:f8b0:4006:80a::2016 AAAA 2607:f8b0:4006:807::201
6703	63.030706	10.0.2.16	142.251.40.138	QUIC	1292	Initial, DCID=a8619ad0592c11f6, PKN: 1, PADDING, CRYPTO, CRYPTO, CRYPTO, PADDING, CRYPTO, PING, PADDING, C
6704	63.033694	10.0.2.16	142.251.40.246	QUIC	1292	Initial, DCID=60053ed939fde81b, PKN: 1, CRYPTO, CRYPTO, PADDING, PING, PADDING, CRYPTO, CRYPTO, PADDING, C
174…	337.778792	10.0.2.16	10.0.2.3	DNS	106	Standard query 0x600b AAAA chromefeedcontentsuggestions-pa.googleapis.com
174…	337.781480	10.0.2.16	10.0.2.3	DNS	79	Standard query 0xe9b2 A static.xx.fbcdn.net
174…	337.781945	10.0.2.16	10.0.2.3	DNS	79	Standard query 0x8a18 AAAA static.xx.fbcdn.net
174…	337.782296	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x0d00 A m.youtube.com
174…	337.782372	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x604a AAAA m.youtube.com
174…	337.798421	10.0.2.3	10.0.2.16	DNS	362	Standard query response 0x9cc9 A chromefeedcontentsuggestions-pa.googleapis.com A 142.250.176.202 A 142.25
174…	337.798544	10.0.2.3	10.0.2.16	DNS	218	Standard query response 0x600b AAAA chromefeedcontentsuggestions-pa.googleapis.com AAAA 2607:f8b0:4006:820
174…	337.802843	10.0.2.3	10.0.2.16	DNS	89	Standard query response 0x0d00 A m.youtube.com A 142.250.80.110
174…	337.802921	10.0.2.3	10.0.2.16	DNS	101	Standard query response 0x604a AAAA m.youtube.com AAAA 2607:f8b0:4006:80d::200e
174…	337.807135	10.0.2.16	10.0.2.3	DNS	91	Standard query 0x867f A images-na.ssl-images-amazon.com
174…	337.809882	10.0.2.16	10.0.2.3	DNS	91	Standard query 0x7299 AAAA images-na.ssl-images-amazon.com
174…	337.810666	10.0.2.16	10.0.2.3	DNS	78	Standard query 0x9466 A en.m.wikipedia.org
174…	337.811753	10.0.2.16	10.0.2.3	DNS	78	Standard query 0x5396 AAAA en.m.wikipedia.org
175…	337.922625	10.0.2.3	10.0.2.16	DNS	130	Standard query response 0x8a18 AAAA static.xx.fbcdn.net CNAME scontent.xx.fbcdn.net AAAA 2a03:2880:f012:10
175…	337.929460	10.0.2.3	10.0.2.16	DNS	118	Standard query response 0xe9b2 A static.xx.fbcdn.net CNAME scontent.xx.fbcdn.net A 157.240.241.1
175…	337.933388	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x2517 A a.espncdn.com
175…	337.935199	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x4379 AAAA a.espncdn.com

The application actively initiates DNS queries to retrieve information from websites like ESPN, Wikipedia, and other advertising services. These queries are likely made to fetch relevant content, including sports updates, general knowledge articles, and advertisements. By accessing these websites, the application aims to provide users with a diverse range of information and services.

APPLICATION SCREENSHOTS



CONCLUSION

The Xlauncher app serves as a secure gateway to users' Android devices, offering a customizable interface that replaces the default home screen. Through various features like theme selection, wallpaper customization, and icon pack options, users can personalize their device's appearance according to their preferences. Additionally, launcher apps often provide tools for organizing installed applications, simplifying navigation with intuitive gesture controls, and optimizing device performance for smoother operation. With built-in features such as app locking and permission controls, Xlauncher ensures user data and privacy remain safeguarded. Importantly, it does not request critical permissions, further enhancing its safety and reliability for users seeking a seamless Android experience.

BENIGN APP 3 – MINDGAMES

The mindgames application offers users convenient access to a wide array of cognitive exercises directly on their smartphones or tablets. Users can engage in stimulating mental activities anytime and anywhere, whether they're commuting, waiting in line, or simply relaxing at home. These applications leverage the touchscreen interface of mobile devices to provide intuitive controls for gameplay, making it easy for users to interact with puzzles and challenges using gestures like tapping, swiping, and dragging.

STATIC ANALYSIS - ANDROWARN


```
                "telephony_identifiers_leakage",
                [
                    "This application reads the ISO country code equivalent of the current registered operator's MCC (Mobile
Country Code)",
                    "This application reads the MCC+MNC of the provider of the SIM",
                    "This application reads the SIM's serial number",
                    "This application reads the current data connection state",
                    "This application reads the device phone type value",
                    "This application reads the numeric name (MCC+MNC) of current registered operator",
                    "This application reads the operator name",
                    "This application reads the phone number string for line 1, for example, the MSISDN for a GSM phone",
                    "This application reads the radio technology (network type) currently in use on the device for data
transmission",
                    "This application reads the unique device ID, i.e the IMEI for GSM and the MEID or ESN for CDMA phones",
                    "This application reads the unique subscriber ID, for example, the IMSI for a GSM phone"
                ]
            ],
```


The analysis of the application highlights significant concerns regarding telephony identifiers leakage, as it accesses various sensitive information pertaining to network and device identifiers. This includes reading the ISO country code equivalent of the current registered operator's Mobile Country Code (MCC), the MCC+MNC of the SIM provider, the SIM's serial number, the device's phone type value, numeric and operator names of the registered operator, phone number string for line 1 (MSISDN), radio technology for data transmission, unique device ID (IMEI, MEID, or ESN), and unique subscriber ID (IMSI). Such access raises substantial privacy and security risks, potentially exposing user and device information to unauthorized parties, necessitating stringent data access controls and compliance measures to mitigate these vulnerabilities effectively.

```
            [
                "connection_interfaces_exfiltration",
                [
                    "This application reads details about the currently active data network",
                    "This application tries to find out if the currently active data network is metered"
                ]
            ],
            [
                "telephony_services_abuse",
                [
                    "This application makes phone calls",
                    "This application sends an SMS message 'v8' to the 'v7' phone number"
                ]
            ],
            [
                "audio_video_eavesdropping",
                []
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address ' returned no addresses for  ; port
is out of range' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address '' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/net/Proxy;-
>type()Ljava/net/Proxy$Type;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'timeout' on the 'N/A' port "
                ]
            ],
            [
                "PIM_data_leakage",
                [
                    "This application accesses the SMS list",
                    "This application accesses data stored in the clipboard"
                ]
            ],
```


- Concerns arise regarding the exfiltration of connection interface details, as the application reads information about the currently active data network and attempts to determine if it is metered.
- There are indications of telephony services abuse, with the application capable of making phone calls and sending an SMS message with specific content to a designated phone number.
- No evidence of audio or video eavesdropping behavior is found in the analysis.
- Suspicious connection establishment is flagged, as the application opens a Socket and connects to remote addresses, including cases where the address is blank or contains unusual string representations.
- PIM (Personal Information Management) data leakage concerns arise, as the application accesses the SMS list and data stored in the clipboard.
- The analysis reveals instances of code execution, including the execution of UNIX commands with various arguments, potentially indicating vulnerabilities or malicious behavior within the application.

```
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.FOREGROUND_SERVICE',\n
'android.permission.INTERNET',\n 'android.permission.POST_NOTIFICATIONS',\n 'android.permission.VIBRATE',\n
'android.permission.WAKE_LOCK',\n 'com.android.vending.BILLING',\n 'com.google.android.c2dm.permission.RECEIVE',\n
'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE',\n 'com.google.android.gms.permission.AD_ID',\n
'mindware.mindgames.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION',\n 'mindware.mindgames.permission.C2D_MESSAGE']",
                    "Implied: []",
                    "Declared: ['mindware.mindgames.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION']"
                ]
            ],
            [
                "features",
                [
                    "android.hardware.touchscreen"
                ]
            ],
            [
                "libraries",
                [
                    "org.apache.http.legacy"
                ]
            ]
```


The application requests a diverse set of permissions, indicating its reliance on various system functionalities and external services. Essential permissions such as ACCESS_NETWORK_STATE and INTERNET suggest network connectivity requirements, crucial for accessing online content and services. The FOREGROUND_SERVICE permission indicates the application's need to run foreground services, possibly for ongoing tasks or background operations. Additionally, permissions like POST_NOTIFICATIONS and VIBRATE suggest the application's ability to deliver notifications and interact with the device's vibration motor.

The inclusion of com.android.vending.BILLING indicates support for in-app purchases, enabling users to make purchases within the application. Permissions related to receiving cloud messages (com.google.android.c2dm.permission.RECEIVE) and binding to install referrer services (com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE) suggest integration with Google Play services for push notifications and app installation tracking. Furthermore, the custom permission mindware.mindgames.

DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION indicates specific functionality or access control tailored to the application's requirements, potentially for dynamic receiver management. Lastly, mindware.mindgames.permission.C2D_MESSAGE implies additional permissions for handling cloud messages. These permissions collectively provide insights into the application's functionalities, interactions with system services, and potential integration with external services.

DYNAMIC ANALYSIS – WIRESHARK

Total number of packets – 62354

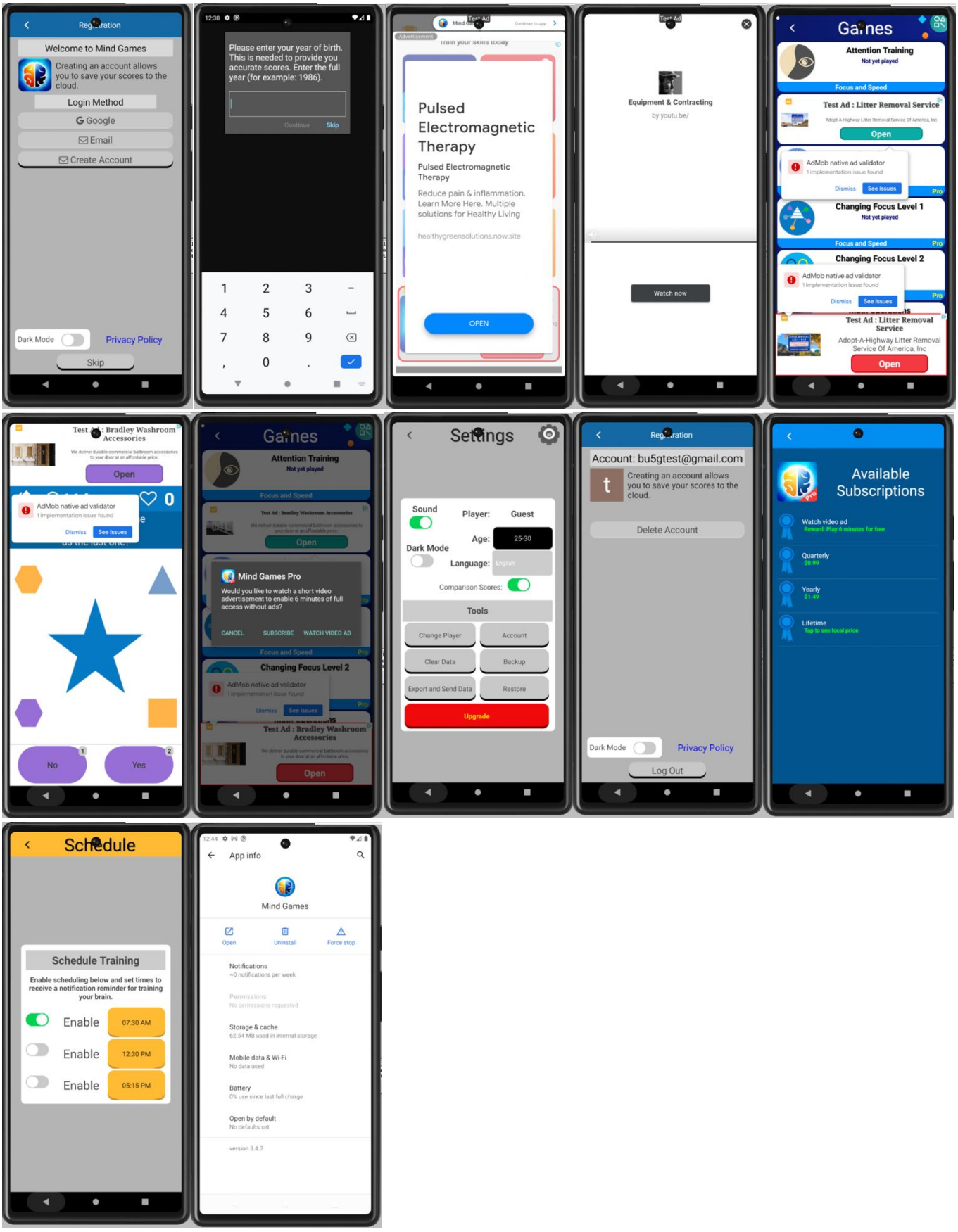
Number of DNS Packets – 938

Number of TCP Packets - 37253

521…	436.456730	10.0.2.3	10.0.2.16	DNS	105	Standard query response 0xf94c A pagead2.googlesyndication.com A 142.250.64.98
574…	447.129153	10.0.2.16	10.0.2.3	DNS	90	Standard query 0xb4e9 AAAA infinitedata-pa.googleapis.com
574…	447.141979	10.0.2.3	10.0.2.16	DNS	202	Standard query response 0xb4e9 AAAA infinitedata-pa.googleapis.com AAAA 2607:f8b0:4006:81f::200a AAAA 2607
574…	447.149585	10.0.2.16	10.0.2.3	DNS	90	Standard query 0x3108 A infinitedata-pa.googleapis.com
574…	447.161682	10.0.2.3	10.0.2.16	DNS	346	Standard query response 0x3108 A infinitedata-pa.googleapis.com A 142.251.40.106 A 142.250.176.202 A 142.2
579…	463.289920	10.0.2.16	10.0.2.3	DNS	80	Standard query 0x2f3d AAAA cm.g.doubleclick.net
579…	463.291861	10.0.2.16	10.0.2.3	DNS	74	Standard query 0x07ec AAAA us-u.openx.net
579…	463.311689	10.0.2.16	10.0.2.3	DNS	88	Standard query 0x8e25 AAAA googleads4.g.doubleclick.net
579…	463.336064	10.0.2.3	10.0.2.16	DNS	140	Standard query response 0x2f3d AAAA cm.g.doubleclick.net SOA ns1.google.com
579…	463.336197	10.0.2.3	10.0.2.16	DNS	148	Standard query response 0x8e25 AAAA googleads4.g.doubleclick.net SOA ns1.google.com
579…	463.336693	10.0.2.16	10.0.2.3	DNS	80	Standard query 0xab61 A cm.g.doubleclick.net
579…	463.336959	10.0.2.16	10.0.2.3	DNS	88	Standard query 0x0a6b A googleads4.g.doubleclick.net
579…	463.337063	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x6d18 AAAA sync.teads.tv
579…	463.349502	10.0.2.3	10.0.2.16	DNS	96	Standard query response 0xab61 A cm.g.doubleclick.net A 142.250.80.2
579…	463.349615	10.0.2.3	10.0.2.16	DNS	104	Standard query response 0x0a6b A googleads4.g.doubleclick.net A 142.250.80.98
579…	463.351417	10.0.2.3	10.0.2.16	DNS	170	Standard query response 0x07ec AAAA us-u.openx.net SOA ns-cloud-c1.googledomains.com
579…	463.352256	10.0.2.16	10.0.2.3	DNS	74	Standard query 0x083e A us-u.openx.net
580…	463.372338	10.0.2.3	10.0.2.16	DNS	106	Standard query response 0x083e A us-u.openx.net A 34.98.64.218 A 35.244.159.8
580…	463.457848	10.0.2.3	10.0.2.16	DNS	225	Standard query response 0x6d18 AAAA sync.teads.tv CNAME sync.teads.tv.edgekey.net CNAME e9957.e4.akamaiedg
580…	463.458512	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x9d2f A sync.teads.tv
580…	463.465701	10.0.2.3	10.0.2.16	DNS	165	Standard query response 0x9d2f A sync.teads.tv CNAME sync.teads.tv.edgekey.net CNAME e9957.e4.akamaiedge.r
582…	480.303230	10.0.2.16	10.0.2.3	DNS	85	Standard query 0xbc88 AAAA lh3.googleusercontent.com
582…	480.315419	10.0.2.3	10.0.2.16	DNS	163	Standard query response 0xbc88 AAAA lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A
582…	480.316031	10.0.2.16	10.0.2.3	DNS	85	Standard query 0x8271 A lh3.googleusercontent.com
582…	480.316702	10.0.2.3	10.0.2.16	DNS	151	Standard query response 0x8271 A lh3.googleusercontent.com CNAME googlehosted.l.googleusercontent.com A 14
583…	514.335880	10.0.2.16	10.0.2.3	DNS	75	Standard query 0xe3ba AAAA mail.google.com
583…	514.348440	10.0.2.3	10.0.2.16	DNS	103	Standard query response 0xe3ba AAAA mail.google.com AAAA 2607:f8b0:4006:809::2005
583…	514.349044	10.0.2.16	10.0.2.3	DNS	75	Standard query 0x6050 A mail.google.com
583…	514.349701	10.0.2.3	10.0.2.16	DNS	91	Standard query response 0x6050 A mail.google.com A 142.250.72.101
583…	514.608777	10.0.2.16	10.0.2.3	DNS	97	Standard query 0x30c0 AAAA mail-attachment.googleusercontent.com
583…	514.621623	10.0.2.3	10.0.2.16	DNS	175	Standard query response 0x30c0 AAAA mail-attachment.googleusercontent.com CNAME googlehosted.l.googleuserc

The application consistently initiates DNS queries to Google Ad Services, indicating its frequent communication with Google's advertising infrastructure. This behavior suggests that the app may be fetching ad content or engaging in ad-related activities provided by Google's advertising platform

APP SCREENSHOTS



CONCLUSION

The mindgames application offers users convenient access to a wide array of cognitive exercises directly on their smartphones or tablets. Users can engage in stimulating mental activities anytime and anywhere, whether they're commuting, waiting in line, or simply relaxing at home. These applications leverage the touchscreen interface of mobile devices to provide intuitive controls for gameplay, making it easy for users to interact with puzzles and challenges using gestures like tapping, swiping, and dragging.

BENIGN APP 4 – RSSDEMON

An RSS blog app is a software application designed to aggregate and display content from various blogs or websites that publish RSS (Really Simple Syndication) feeds. This application allow users to subscribe to their favorite blogs or websites and receive updates in a centralized location, typically within the app itself. Users can browse through the latest articles, posts, or news items from multiple sources without having to visit each website individually. RSSDemon provides features such as customization options for organizing and categorizing feeds, offline reading capabilities, notifications for new updates, and the ability to save or share interesting articles. Overall, these apps offer a convenient way for users to stay informed and up-to-date with the latest content from their preferred online sources.

STATIC ANALYSIS – ANDROWARN

```
                "telephony_identifiers_leakage",
                [
                    "This application reads the ISO country code equivalent for the SIM provider's country code",
                    "This application reads the ISO country code equivalent of the current registered operator's MCC (Mobile
Country Code)",
                    "This application reads the MCC+MNC of the provider of the SIM",
                    "This application reads the device phone type value",
                    "This application reads the numeric name (MCC+MNC) of current registered operator",
                    "This application reads the radio technology (network type) currently in use on the device for data
transmission"
                ]
```

The analysis reveals that the application exhibits telephony identifiers leakage, accessing sensitive information related to telecommunication services. Specifically, it reads the ISO country code equivalent for the SIM provider's country code, the ISO country code equivalent of the current registered operator's Mobile Country Code (MCC), and the MCC+MNC (Mobile Country Code + Mobile Network Code) of the SIM provider. Additionally, the application retrieves the device's phone type value, the numeric name (MCC+MNC) of the current registered operator, and the radio technology (network type) currently in use on the device for data transmission. Such access to telephony identifiers raises significant privacy concerns and underscores the importance of implementing stringent data access controls and compliance measures to safeguard user privacy.

```
            [
                "connection_interfaces_exfiltration",
                [
                    "This application reads details about the currently active data network",
                    "This application tries to find out if the currently active data network is metered"
                ]
            ],
            [
                "telephony_services_abuse",
                [
                    "This application makes phone calls"
                ]
            ],
            [
                "audio_video_eavesdropping",
                []
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address ' returned no addresses for  ; port
is out of range' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address '' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/net/Proxy;-
>type()Ljava/net/Proxy$Type;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'timeout' on the 'N/A' port "
                ]
            ],
            [
                "PIM_data_leakage",
                [
                    "This application accesses the downloads folder",
                    "This application accesses data stored in the clipboard"
                ]
            ],
```


- The analysis indicates potential connection interfaces exfiltration, as the application reads details about the currently active data network and attempts to determine if it is metered.
- Telephony services abuse is flagged, with the application capable of making phone calls.
- No evidence of audio or video eavesdropping behavior is found in the analysis.
- Suspicious connection establishment is noted, as the application opens a Socket and connects to remote addresses, including cases where the address is blank or contains unusual string representations.
- Concerns arise regarding PIM (Personal Information Management) data leakage, as the application accesses the downloads folder and data stored in the clipboard.

```
                "providers",
                [
                    "androidx.core.content.FileProvider",
                    "com.appyet.provider.SuggestionProvider",
                    "com.just.agentweb.AgentWebFileProvider",
                    "com.facebook.ads.AudienceNetworkContentProvider",
                    "com.google.firebase.provider.FirebaseInitProvider",
                    "com.google.android.gms.ads.MobileAdsInitProvider",
                    "androidx.startup.InitializationProvider"
                ]
            ],
            [
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.FLASHLIGHT',\n 'android.permission.FOREGROUND_SERVICE',\n 'android.permission.INTERNET',\n
'android.permission.POST_NOTIFICATIONS',\n 'android.permission.READ_EXTERNAL_STORAGE',\n
'android.permission.RECEIVE_BOOT_COMPLETED',\n 'android.permission.VIBRATE',\n 'android.permission.WAKE_LOCK',\n
'android.permission.WRITE_EXTERNAL_STORAGE',\n 'com.google.android.c2dm.permission.RECEIVE',\n
'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE',\n 'com.google.android.gms.permission.AD_ID',\n
'com.samsung.android.providers.context.permission.WRITE_USE_APP_FEATURE_SURVEY']",
                    "Implied: []",
                    "Declared: []"
                ]
            ],
            [
                "features",
                [
                    "android.hardware.location.network",
                    "android.hardware.touchscreen",
                    "android.hardware.wifi"
                ]
            ],
            [
                "libraries",
                [
                    "androidx.window.extensions",
                    "androidx.window.sidecar"
                ]
            ]
        ]
```


The providers likely facilitate access to shared files, suggestions, web content, advertising data, Firebase services, Google Mobile Ads, and startup initialization processes.

In terms of permissions, the application requests a range of permissions necessary for its functionalities, including access to network state and WiFi information, flashlight control, internet access, foreground service usage, notification posting, storage access, boot completion reception, vibration control, wake lock, and app feature survey writing permissions for Samsung devices. Notably, no custom permissions are declared, implying reliance on standard Android permissions.

The application features hardware support for network location, touchscreen input, and WiFi connectivity. Additionally, it utilizes the androidx.window.extensions and androidx.window.sidecar libraries, possibly for window management and UI enhancements. These components collectively contribute to the application's functionality and feature set, providing insights into its capabilities and potential interactions with system resources and external services.

DYNAMIC ANALYSIS – WIRESHARK

Total Packets Traced : 130394 Packets

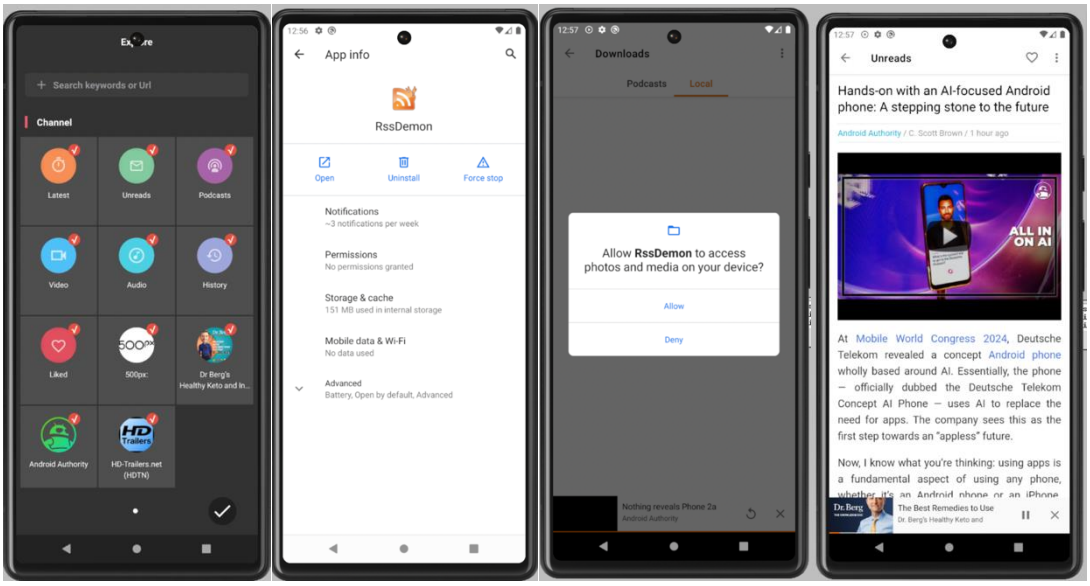
DNS Packets : 842 Packets

TCP Packets : 114671 Packets

115…	335.555966	10.0.2.16	10.0.2.3	DNS	80	Standard query 0x22e4 A feeds.feedburner.com
115…	335.568530	10.0.2.3	10.0.2.16	DNS	127	Standard query response 0x22e4 A feeds.feedburner.com CNAME www4.l.google.com A 142.250.65.174
115…	335.587321	10.0.2.3	10.0.2.16	DNS	147	Standard query response 0x0645 AAAA feed.500px.com CNAME q584q1.feedproxy.ghs.google.com AAAA 2607:f8b0:4
115…	335.588471	10.0.2.16	10.0.2.3	DNS	74	Standard query 0x12df A feed.500px.com
115…	335.601061	10.0.2.3	10.0.2.16	DNS	135	Standard query response 0x12df A feed.500px.com CNAME q584q1.feedproxy.ghs.google.com A 142.251.40.179
115…	335.779408	10.0.2.3	10.0.2.16	DNS	195	Standard query response 0x1228 AAAA feeds.hd-trailers.net CNAME redirect.feedpress.me SOA charles.ns.clouc
115…	335.780167	10.0.2.16	10.0.2.3	DNS	81	Standard query 0xeecc A feeds.hd-trailers.net
115…	335.788196	10.0.2.3	10.0.2.16	DNS	132	Standard query response 0xeecc A feeds.hd-trailers.net CNAME redirect.feedpress.me A 5.135.16.50
115…	335.903719	10.0.2.16	10.0.2.3	DNS	84	Standard query 0xdb7a AAAA www.androidauthority.com
115…	335.933540	10.0.2.3	10.0.2.16	DNS	168	Standard query response 0xdb7a AAAA www.androidauthority.com AAAA 2606:4700:10::ac43:210 AAAA 2606:4700:1
115…	335.934291	10.0.2.16	10.0.2.3	DNS	84	Standard query 0xbacd A www.androidauthority.com
115…	335.942198	10.0.2.3	10.0.2.16	DNS	132	Standard query response 0xbacd A www.androidauthority.com A 172.67.2.16 A 104.20.85.39 A 104.20.84.39
115…	336.479348	10.0.2.16	10.0.2.3	DNS	76	Standard query 0x3b7f AAAA drscdn.500px.org
115…	336.522152	10.0.2.16	10.0.2.3	DNS	76	Standard query 0x1292 AAAA drscdn.500px.org
115…	336.582697	10.0.2.16	10.0.2.3	DNS	84	Standard query 0x6aef AAAA androidauth.wpengine.com
115…	336.612536	10.0.2.3	10.0.2.16	DNS	159	Standard query response 0x6aef AAAA androidauth.wpengine.com SOA jim.ns.cloudflare.com
115…	336.613265	10.0.2.16	10.0.2.3	DNS	84	Standard query 0x3d72 A androidauth.wpengine.com
115…	336.621020	10.0.2.3	10.0.2.16	DNS	100	Standard query response 0x3d72 A androidauth.wpengine.com A 34.123.130.65
115…	336.716894	10.0.2.3	10.0.2.16	DNS	343	Standard query response 0x1292 AAAA drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net AAAA 2600:9000:21
115…	336.716957	10.0.2.3	10.0.2.16	DNS	343	Standard query response 0x3b7f AAAA drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net AAAA 2600:9000:21
115…	336.717666	10.0.2.16	10.0.2.3	DNS	76	Standard query 0x2ce2 A drscdn.500px.org
115…	336.724070	10.0.2.16	10.0.2.3	DNS	76	Standard query 0x7d5b A drscdn.500px.org
115…	336.753298	10.0.2.3	10.0.2.16	DNS	183	Standard query response 0x7d5b A drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net A 13.225.214.41 A 13
115…	336.753372	10.0.2.3	10.0.2.16	DNS	183	Standard query response 0x2ce2 A drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net A 13.225.214.34 A 13
116…	349.898602	10.0.2.16	10.0.2.3	DNS	69	Standard query 0x7a46 AAAA anchor.fm
116…	350.101098	10.0.2.3	10.0.2.16	DNS	153	Standard query response 0x7a46 AAAA anchor.fm SOA ns-533.awsdns-02.net
116…	350.101603	10.0.2.16	10.0.2.3	DNS	69	Standard query 0x3a34 A anchor.fm
116…	350.123357	10.0.2.3	10.0.2.16	DNS	133	Standard query response 0x3a34 A anchor.fm A 151.101.66.133 A 151.101.130.133 A 151.101.194.133 A 151.101.
116…	350.362921	10.0.2.16	10.0.2.3	DNS	81	Standard query 0xad07 AAAA imasdk.googleapis.com
116…	350.375239	10.0.2.3	10.0.2.16	DNS	109	Standard query response 0xad07 AAAA imasdk.googleapis.com AAAA 2607:f8b0:4006:816::200a
116…	350.375587	10.0.2.16	10.0.2.3	DNS	81	Standard query 0xc0cc A imasdk.googleapis.com
116…	350.388093	10.0.2.3	10.0.2.16	DNS	97	Standard query response 0xc0cc A imasdk.googleapis.com A 142.250.65.234
116…	350.689814	10.0.2.16	10.0.2.3	DNS	81	Standard query 0xfee1 AAAA bid.g.doubleclick.net

The app generates DNS queries directed towards platforms like feeds.hd-trailers.net, anchor.fm, and other advertising services websites. This indicates that the application may be fetching data or content from these sources, potentially for displaying advertisements or accessing multimedia content.

APP SCREENSHOTS



CONCLUSION

This application ensures user safety by abstaining from requesting critical permissions, thereby safeguarding sensitive data and device integrity. Users can confidently subscribe to their preferred blogs or websites, receiving updates securely within the app itself. With customizable features for organizing and categorizing feeds, offline reading capabilities, and notifications for new updates, the app prioritizes user privacy and security. Its stringent adherence to limited permissions underscores its commitment to providing a secure browsing experience, empowering users to stay informed without compromising their personal information or device security.

BENIGN APP 5 – Prayer App

The mobile application is designed to facilitate and enhance users' spiritual practices by offering a range of features aimed at prayer, meditation, and spiritual growth. The app provides users with access to various prayers, meditation guides, and scripture readings, allowing them to engage in spiritual practices anytime, anywhere. Additionally, prayer apps include tools for organizing prayer lists, setting reminders and, enabling users to maintain a consistent prayer routine and connect with others for support and encouragement in their faith journey

STATIC ANALYSIS - ANDROGAURD

```
[
    "telephony_identifiers_leakage",
    []
],
```

The application does not access or leak any telephony identifiers.

```
            [
                "location_lookup",
                [
                    "This application reads location information from all available providers (WiFi, GPS etc.)"
                ]
            ],
            [
                "connection_interfaces_exfiltration",
                [
                    "This application reads details about the currently active data network",
                    "This application tries to find out if the currently active data network is metered"
                ]
            ],
            [
                "telephony_services_abuse",
                [
                    "This application makes phone calls"
                ]
            ],
            [
                "audio_video_eavesdropping",
                [
                    "This application records audio from the 'MIC' source "
                ]
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address '4' on the 'v31' port "
                ]
            ],
            [
                "PIM_data_leakage",
                [
                    "This application accesses the contacts list"
                ]
            ],
            [
                "code_execution",
                [
                    "This application executes a UNIX command",
                    "This application executes a UNIX command containing this argument: 'getprop'"
                ]
            ]
        ]
```

The analyzed application exhibits concerning behavior across several fronts. It actively retrieves location information from various sources, including WiFi and GPS, potentially compromising user privacy. Moreover, it accesses detailed information about the current data network and attempts to ascertain whether it is metered,

suggesting possible data exfiltration intentions. Additionally, the app possesses the capability to initiate phone calls autonomously, raising alarms regarding potential abuse of telephony services. Furthermore, it can surreptitiously record audio from the device's microphone, posing a serious threat to user confidentiality. This combination of intrusive functionalities, including unauthorized data network scrutiny, telephony misuse, and audio eavesdropping, underscores significant privacy and security risks associated with the application.


```
            [
                "providers",
                [
                    "androidx.core.content.FileProvider"
                ]
            ],
            [
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_COARSE_LOCATION',\n 'android.permission.ACCESS_FINE_LOCATION',\n
'android.permission.ACCESS_LOCATION_EXTRA_COMMANDS',\n 'android.permission.ACCESS_MOCK_LOCATION',\n
'android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.CHANGE_WIFI_STATE',\n 'android.permission.INTERNET']",
                    "Implied: []",
                    "Declared: []"
                ]
            ],
            [
                "features",
                []
            ],
            [
                "libraries",
                [
                    "org.apache.http.legacy"
                ]
            ]
        ]
```

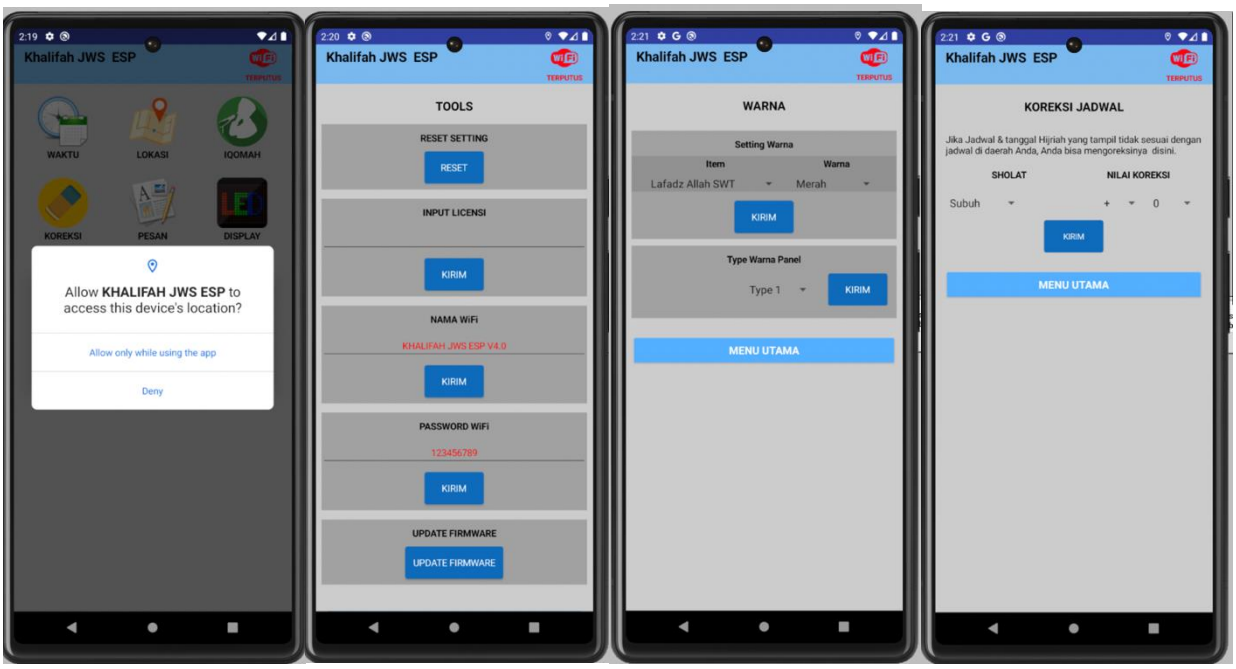

The application requests a wide range of location-related permissions, including access to coarse and fine location data, commands for location access, and the ability to detect mock locations. Additionally, it seeks permissions to access network and Wi-Fi states and change Wi-Fi settings. These permissions grant the app extensive control over location services and network connectivity, raising concerns about potential privacy violations and unauthorized data collection. Furthermore, the presence of the org.apache.http.legacy library suggests that the app may utilize outdated HTTP communication methods, potentially exposing users to security vulnerabilities associated with deprecated APIs.

DYNAMIC ANALYSIS – WIRESHARK
Total Packets Traced : 122199 Packets
DNS Packets : 440 Packets
TCP Packets : 9378 Packets

115…	336.621020	10.0.2.3	10.0.2.16	DNS	100	Standard query response 0x3d72 A androidauth.wpengine.com A 34.123.130.65
115…	336.716894	10.0.2.3	10.0.2.16	DNS	343	Standard query response 0x1292 AAAA drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net AAAA 2600:9000:21
115…	336.716957	10.0.2.3	10.0.2.16	DNS	343	Standard query response 0x3b7f AAAA drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net AAAA 2600:9000:21
115…	336.717666	10.0.2.16	10.0.2.3	DNS	76	Standard query 0x2ce2 A drscdn.500px.org
115…	336.724070	10.0.2.16	10.0.2.3	DNS	76	Standard query 0x7d5b A drscdn.500px.org
115…	336.753298	10.0.2.3	10.0.2.16	DNS	183	Standard query response 0x7d5b A drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net A 13.225.214.41 A 13
115…	336.753372	10.0.2.3	10.0.2.16	DNS	183	Standard query response 0x2ce2 A drscdn.500px.org CNAME d23koxhuryc6ae.cloudfront.net A 13.225.214.34 A 13
116…	349.898602	10.0.2.16	10.0.2.3	DNS	69	Standard query 0x7a46 AAAA anchor.fm
116…	350.101098	10.0.2.3	10.0.2.16	DNS	153	Standard query response 0x7a46 AAAA anchor.fm SOA ns-533.awsdns-02.net
116…	350.101603	10.0.2.16	10.0.2.3	DNS	69	Standard query 0x3a34 A anchor.fm
116…	350.123357	10.0.2.3	10.0.2.16	DNS	133	Standard query response 0x3a34 A anchor.fm A 151.101.66.133 A 151.101.130.133 A 151.101.194.133 A 151.101.
116…	350.362921	10.0.2.16	10.0.2.3	DNS	81	Standard query 0xad07 AAAA imasdk.googleapis.com
116…	350.375239	10.0.2.3	10.0.2.16	DNS	109	Standard query response 0xad07 AAAA imasdk.googleapis.com AAAA 2607:f8b0:4006:816::200a
116…	350.375587	10.0.2.16	10.0.2.3	DNS	81	Standard query 0xc0cc A imasdk.googleapis.com
116…	350.388093	10.0.2.3	10.0.2.16	DNS	97	Standard query response 0xc0cc A imasdk.googleapis.com A 142.250.65.234
116…	350.689814	10.0.2.16	10.0.2.3	DNS	81	Standard query 0xfee1 AAAA bid.g.doubleclick.net
116…	350.702511	10.0.2.3	10.0.2.16	DNS	141	Standard query response 0xfee1 AAAA bid.g.doubleclick.net SOA ns1.google.com
116…	350.716318	10.0.2.16	10.0.2.3	DNS	81	Standard query 0x261b A bid.g.doubleclick.net
116…	350.729049	10.0.2.3	10.0.2.16	DNS	337	Standard query response 0x261b A bid.g.doubleclick.net A 142.251.167.155 A 142.251.179.157 A 172.253.115.1
116…	350.893681	10.0.2.16	10.0.2.3	DNS	75	Standard query 0x6ec9 AAAA csi.gstatic.com
116…	350.906255	10.0.2.3	10.0.2.16	DNS	131	Standard query response 0x6ec9 AAAA csi.gstatic.com AAAA 2404:6800:4003:c0f::5e AAAA 2404:6800:4003:c0f::7
116…	350.906738	10.0.2.16	10.0.2.3	DNS	75	Standard query 0x447c A csi.gstatic.com
116…	350.919053	10.0.2.3	10.0.2.16	DNS	91	Standard query response 0x447c A csi.gstatic.com A 216.239.32.3
116…	351.165194	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x2f3b AAAA gcdn.2mdn.net
116…	351.199609	10.0.2.3	10.0.2.16	DNS	101	Standard query response 0x2f3b AAAA gcdn.2mdn.net AAAA 2607:f8b0:4006:821::200e
116…	351.200270	10.0.2.16	10.0.2.3	DNS	73	Standard query 0x5e01 A gcdn.2mdn.net
116…	351.212915	10.0.2.3	10.0.2.16	DNS	89	Standard query response 0x5e01 A gcdn.2mdn.net A 142.251.40.174
116…	351.354725	10.0.2.16	10.0.2.3	DNS	87	Standard query 0x2275 AAAA r2---sn-ab5l6nr6.c.2mdn.net
116…	351.402020	10.0.2.3	10.0.2.16	DNS	154	Standard query response 0x2275 AAAA r2---sn-ab5l6nr6.c.2mdn.net CNAME r2.sn-ab5l6nr6.c.2mdn.net AAAA 2607:

The application actively sends DNS queries to Google ad services, indicating its active retrieval of data or content from these sources. This behavior suggests that the application may be obtaining information for the purpose of displaying advertisements or accessing multimedia content associated with these ad services. This could involve loading ad banners, video ads, or other promotional material within the app's interface

APPLICATION SCREENSHOTS



CONCLUSION

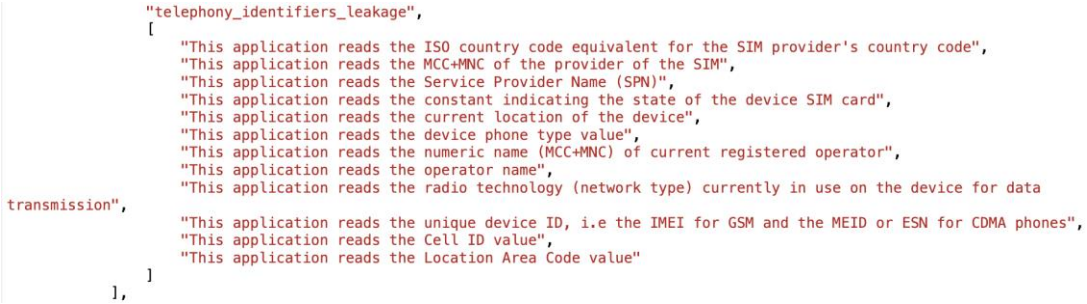
The mobile application doesn't request critical permissions is significant. Critical permissions typically grant access to sensitive user data or device functionality, and apps that don't require them pose fewer security risks. Additionally, by not violating user data, the application ensures that users can engage with its features without compromising their privacy or exposing personal information.

MALWARE APPS

MALWARE APP 1 - SUPER CLEANER - ANTIVIRUS HACK

Super Cleaner - Antivirus Hack app is a mobile application designed to safeguard devices from malware and viruses while optimizing performance by removing unnecessary files and processes. Through features like virus scanning and real-time protection, these apps actively defend against malicious software, ensuring the security of users' devices. Additionally, they offer tools for cleaning up junk files, managing installed applications, and optimizing battery usage, enhancing device performance and extending battery life. With privacy protection features to safeguard sensitive data and prevent unauthorized access, antivirus cleaner apps provide users with a comprehensive solution to maintain the security and efficiency of their mobile devices.

STATIC ANALYSIS - ANDROWARN



```
                "telephony_identifiers_leakage",
                [
                    "This application reads the ISO country code equivalent for the SIM provider's country code",
                    "This application reads the MCC+MNC of the provider of the SIM",
                    "This application reads the Service Provider Name (SPN)",
                    "This application reads the constant indicating the state of the device SIM card",
                    "This application reads the current location of the device",
                    "This application reads the device phone type value",
                    "This application reads the numeric name (MCC+MNC) of current registered operator",
                    "This application reads the operator name",
                    "This application reads the radio technology (network type) currently in use on the device for data
transmission",
                    "This application reads the unique device ID, i.e the IMEI for GSM and the MEID or ESN for CDMA phones",
                    "This application reads the Cell ID value",
                    "This application reads the Location Area Code value"
                ]
            ],
```

The analysis of the application reveals concerning telephony identifiers leakage, as it accesses various sensitive information related to telecommunication services. Specifically, the application reads the ISO country code equivalent for the SIM provider's country code, the MCC+MNC (Mobile Country Code + Mobile Network Code) of the SIM provider, the Service Provider Name (SPN), the constant indicating the state of the device SIM card, and the current location of the device. Furthermore, it retrieves the device phone type value, the numeric name (MCC+MNC) of the current registered operator, and the operator name. Additionally, the application accesses the radio technology (network type) currently in use on the device for data transmission, the unique device ID (IMEI for GSM and the MEID or ESN for CDMA phones), the Cell ID value, and the Location Area Code value. the application's access to IMEI and MEID poses substantial privacy risks, potentially enabling tracking and profiling of individual devices. Such extensive access to telephony identifiers raises significant privacy concerns and underscores the importance of implementing stringent data access controls and compliance measures to safeguard user privacy.

```
                "location_lookup",
                [
                    "This application reads location information from all available providers (WiFi, GPS etc.)"
                ]
            ],
            [
                "connection_interfaces_exfiltration",
                [
                    "This application reads details about the currently active data network",
                    "This application tries to find out if the currently active data network is metered"
                ]
            ],
            [
                "telephony_services_abuse",
                []
            ],
            [
                "audio_video_eavesdropping",
                []
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address '' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/net/Proxy;-
>type()Ljava/net/Proxy$Type;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'timeout' on the 'N/A' port "
                ]
            ],
            [
                "PIM_data_leakage",
                []
            ],
```


The analysis reveals several concerning behaviors within the application. Firstly, it conducts location lookups by reading location information from all available providers, including WiFi and GPS. Additionally, the application engages in connection interfaces exfiltration, accessing details about the currently active data network and attempting to determine if it is metered. Furthermore, suspicious connection establishment is flagged, as the application opens sockets and connects to remote addresses, including cases where the address is blank or contains unusual string representations.

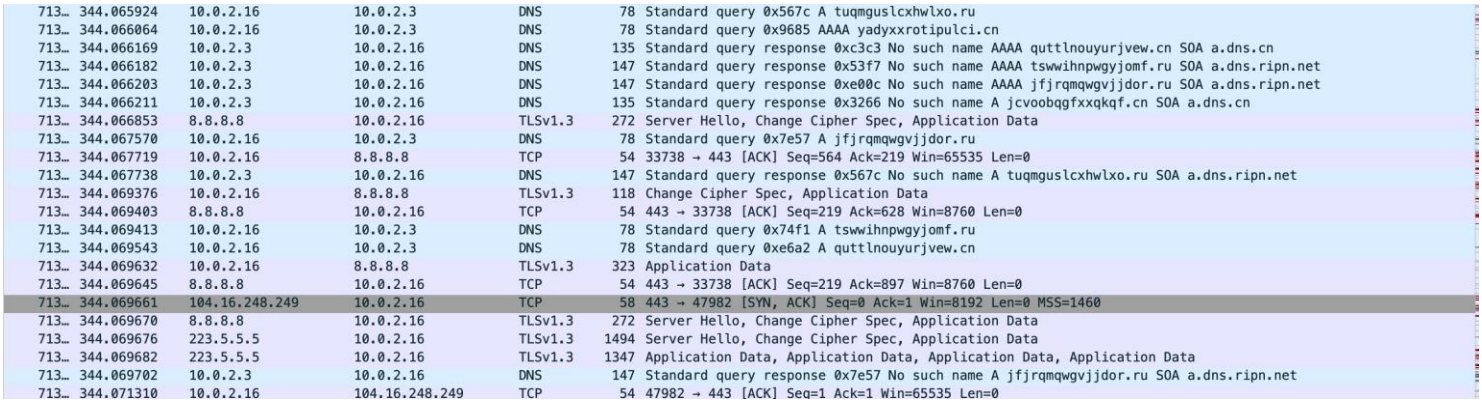

```
            [
                "providers",
                [
                    "com.google.firebase.provider.FirebaseInitProvider"
                ]
            ],
            [
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.FOREGROUND_SERVICE',\n 'android.permission.GET_TASKS',\n 'android.permission.INTERNET',\n
'android.permission.QUICKBOOT_POWERON',\n 'android.permission.READ_APP_BADGE',\n 'android.permission.RECEIVE_BOOT_COMPLETED',\n
'android.permission.SEND_SMS',\n 'android.permission.SYSTEM_ALERT_WINDOW',\n 'android.permission.VIBRATE',\n
'android.permission.WAKE_LOCK',\n 'com.anddoes.launcher.permission.UPDATE_COUNT',\n
'com.apps.go.clean.boost.master.hack.permission.C2D_MESSAGE',\n 'com.google.android.c2dm.permission.RECEIVE',\n
'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE',\n 'com.htc.launcher.permission.READ_SETTINGS',\n
'com.htc.launcher.permission.UPDATE_SHORTCUT',\n 'com.huawei.android.launcher.permission.CHANGE_BADGE',\n
'com.huawei.android.launcher.permission.READ_SETTINGS',\n 'com.huawei.android.launcher.permission.WRITE_SETTINGS',\n
'com.majeur.launcher.permission.UPDATE_BADGE',\n 'com.oppo.launcher.permission.READ_SETTINGS',\n
'com.oppo.launcher.permission.WRITE_SETTINGS',\n 'com.sec.android.provider.badge.permission.READ',\n
'com.sec.android.provider.badge.permission.WRITE',\n 'com.sonyericsson.home.permission.BROADCAST_BADGE',\n
'com.sonymobile.home.permission.PROVIDER_INSERT_BADGE',\n 'me.everything.badger.permission.BADGE_COUNT_READ',\n
'me.everything.badger.permission.BADGE_COUNT_WRITE']",
                    "Implied: []",
                    "Declared: ['com.apps.go.clean.boost.master.hack.permission.C2D_MESSAGE']"
                ]
            ],
```


The application's behavior of sending SMS to premium numbers without user consent poses a serious threat to user privacy and financial security. This unauthorized action aligns with the permissions requested by the

application, particularly the permission to send SMS messages **(android.permission.SEND_SMS)**. By leveraging this permission alongside others like **INTERNET** and **RECEIVE_BOOT_COMPLETED**, the application can autonomously initiate SMS messages to premium numbers, potentially resulting in unexpected charges for users.

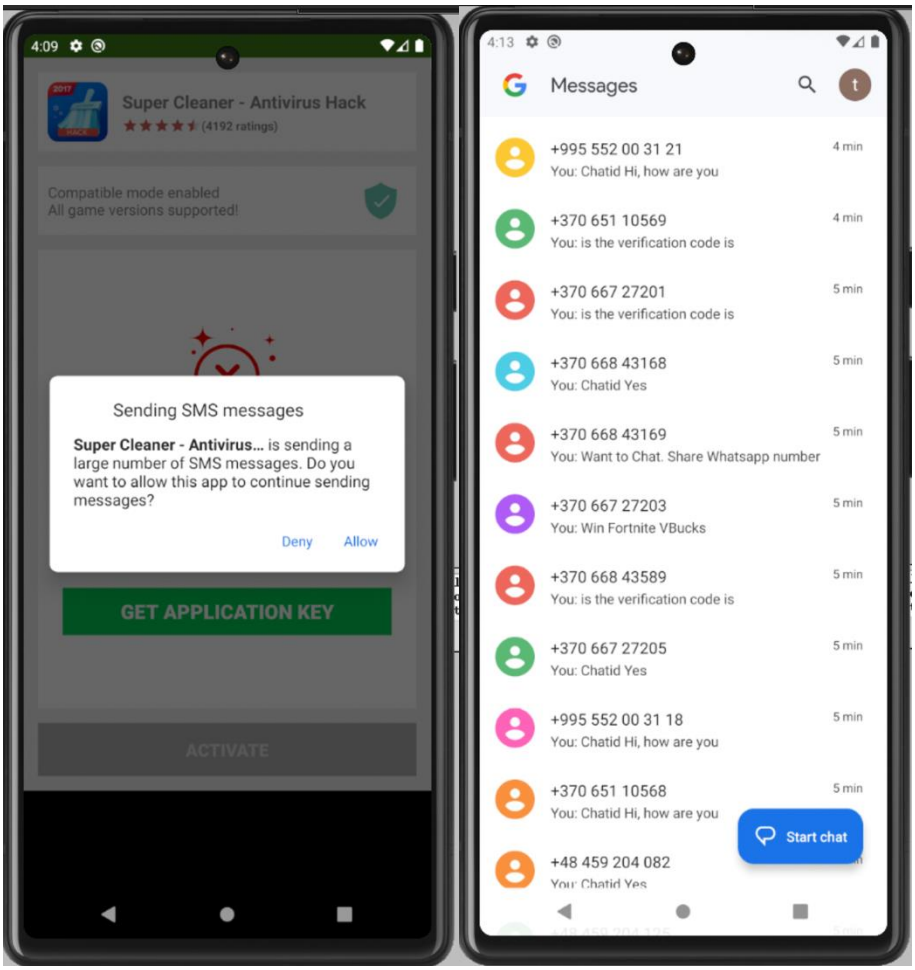
DYNAMIC ANALYSIS – WIRESHARK

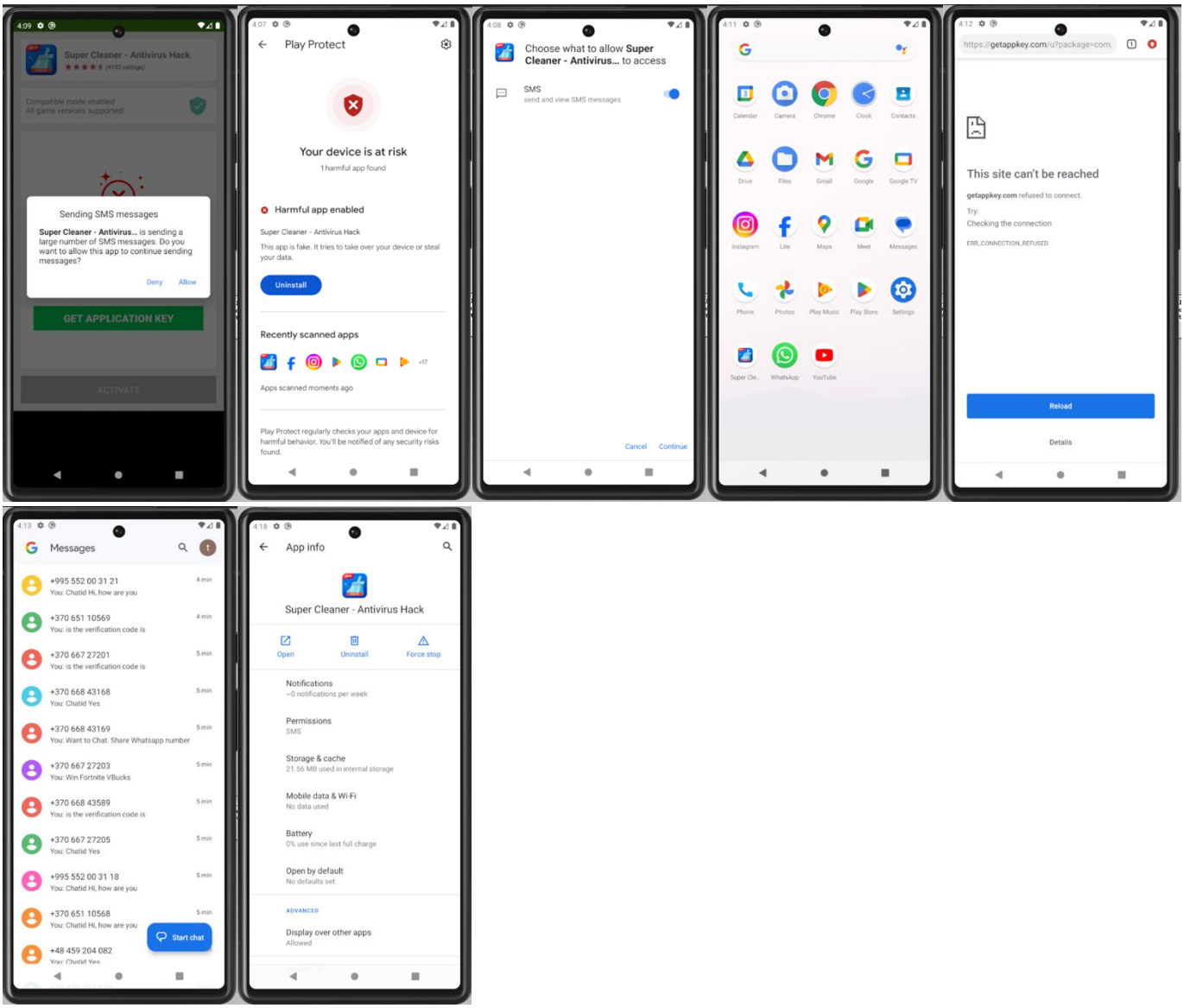
Total Packets Traced : 156897 Packets
DNS Packets : 1060 Packets
TCP Packets : 7190 Packets
ICMP Packets : 417 Packets



713…	344.065924	10.0.2.16	10.0.2.3	DNS	78	Standard query 0x567c A tuqmguslcxhwlxo.ru
713…	344.066064	10.0.2.16	10.0.2.3	DNS	78	Standard query 0x9685 AAAA yadyxxrotipulci.cn
713…	344.066169	10.0.2.3	10.0.2.16	DNS	135	Standard query response 0xc3c3 No such name AAAA quttlnouyurjvew.cn SOA a.dns.cn
713…	344.066182	10.0.2.3	10.0.2.16	DNS	147	Standard query response 0x53f7 No such name AAAA tswwihnpwgyjomf.ru SOA a.dns.ripn.net
713…	344.066203	10.0.2.3	10.0.2.16	DNS	147	Standard query response 0xe00c No such name AAAA jfjrqmqwgvjjdor.ru SOA a.dns.ripn.net
713…	344.066211	10.0.2.3	10.0.2.16	DNS	135	Standard query response 0x3266 No such name A jcvoobqgfxxqkqf.cn SOA a.dns.cn
713…	344.066853	8.8.8.8	10.0.2.16	TLSv1.3	272	Server Hello, Change Cipher Spec, Application Data
713…	344.067570	10.0.2.16	10.0.2.3	DNS	78	Standard query 0x7e57 A jfjrqmqwgvjjdor.ru
713…	344.067719	10.0.2.16	8.8.8.8	TCP	54	33738 → 443 [ACK] Seq=564 Ack=219 Win=65535 Len=0
713…	344.067738	10.0.2.3	10.0.2.16	DNS	147	Standard query response 0x567c No such name A tuqmguslcxhwlxo.ru SOA a.dns.ripn.net
713…	344.069376	10.0.2.16	8.8.8.8	TLSv1.3	118	Change Cipher Spec, Application Data
713…	344.069403	8.8.8.8	10.0.2.16	TCP	54	443 → 33738 [ACK] Seq=219 Ack=628 Win=8760 Len=0
713…	344.069413	10.0.2.16	10.0.2.3	DNS	78	Standard query 0x74f1 A tswwihnpwgyjomf.ru
713…	344.069543	10.0.2.16	10.0.2.3	DNS	78	Standard query 0xe6a2 A quttlnouyurjvew.cn
713…	344.069632	10.0.2.16	8.8.8.8	TLSv1.3	323	Application Data
713…	344.069645	8.8.8.8	10.0.2.16	TCP	54	443 → 33738 [ACK] Seq=219 Ack=897 Win=8760 Len=0
713…	344.069661	104.16.248.249	10.0.2.16	TCP	58	443 → 47982 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
713…	344.069670	8.8.8.8	10.0.2.16	TLSv1.3	272	Server Hello, Change Cipher Spec, Application Data
713…	344.069676	223.5.5.5	10.0.2.16	TLSv1.3	1494	Server Hello, Change Cipher Spec, Application Data
713…	344.069682	223.5.5.5	10.0.2.16	TLSv1.3	1347	Application Data, Application Data, Application Data, Application Data
713…	344.069702	10.0.2.3	10.0.2.16	DNS	147	Standard query response 0x7e57 No such name A jfjrqmqwgvjjdor.ru SOA a.dns.ripn.net
713…	344.071310	10.0.2.16	104.16.248.249	TCP	54	47982 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0

The application is noted for generating DNS queries aimed at dubious websites (tswwihnpwgyjomf.ru, quttlnouyurjvew, and more), raising apprehensions regarding potential security vulnerabilities associated with accessing unreliable or suspicious domains. Such behavior exposes users to a range of threats, including malware dissemination, phishing schemes, and unauthorized data breaches. To bolster security protocols, it is recommended to closely monitor and restrict the application's DNS queries, implement robust domain filtering mechanisms, and employ stringent network security protocols to block access to untrusted websites and mitigate potential risks. Additionally, educating users on prudent browsing practices and the imperative of avoiding interactions with dubious domains can significantly enhance overall cybersecurity resilience.


4:09
Super Cleaner - Antivirus Hack
(4192 ratings)
Compatible mode enabled
All game versions supported!
Sending SMS messages
Super Cleaner - Antivirus... is sending a large number of SMS messages. Do you want to allow this app to continue sending messages?
Deny
Allow
GET APPLICATION KEY
ACTIVATE
4:13
Messages
+995 552 00 31 21
You: Chatid Hi, how are you
4 min
+370 651 10569
You: is the verification code is
4 min
+370 667 27201
You: is the verification code is
5 min
+370 668 43168
You: Chatid Yes
5 min
+370 668 43169
You: Want to Chat. Share Whatsapp number
5 min
+370 667 27203
You: Win Fortnite VBucks
5 min
+370 668 43589
You: is the verification code is
5 min
+370 667 27205
You: Chatid Yes
5 min
+995 552 00 31 18
You: Chatid Hi, how are you
5 min
+370 651 10568
You: Chatid Hi, how are you
5 min
Start chat
+48 459 204 082
You: Chatid Yes



CONCLUSION

The application egregiously violates user permissions by illicitly utilizing the user's device to send SMS messages to premium numbers without explicit consent, thereby potentially incurring additional costs for the user. This unauthorized behavior is facilitated by the permissions granted to the application, which include the ability to read SMS messages, send SMS messages, and operate background processes. By exploiting these permissions, the application bypasses the user's control over their device, potentially resulting in unexpected charges and privacy breaches. Such actions undermine user trust and raise significant concerns regarding the application's integrity and adherence to ethical standards.

MALWARE APP 2 – VIDEO TRANSCODER

STATIC ANALYSIS - ANDROWARN


```
                "telephony_identifiers_leakage",
                [
                    "This application reads the MCC+MNC of the provider of the SIM",
                    "This application reads the Service Provider Name (SPN)",
                    "This application reads the constant indicating the state of the device SIM card",
                    "This application reads the device phone type value",
                    "This application reads the numeric name (MCC+MNC) of current registered operator",
                    "This application reads the operator name",
                    "This application reads the phone's current state",
                    "This application reads the radio technology (network type) currently in use on the device for data
transmission",
                    "This application reads the unique device ID, i.e the IMEI for GSM and the MEID or ESN for CDMA phones"
                ]
            ],
```


The "telephony_identifiers_leakage" threat in the application exposes a range of sensitive information related to telephony identifiers. This includes reading the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the SIM provider, accessing the Service Provider Name (SPN), retrieving the device's SIM card state, phone type value, current operator's numeric name, and operator name. Additionally, it reads the phone's current state and radio technology (network type) used for data transmission. Most critically, the application accesses the unique device ID, such as the International Mobile Equipment Identity (IMEI) for GSM devices and the Mobile Equipment Identifier (MEID) or Electronic Serial Number (ESN) for CDMA phones. This exposes users to potential privacy risks and underscores the importance of safeguarding telephony identifiers against unauthorized access.


```
            [
                "location_lookup",
                []
            ],
            [
                "connection_interfaces_exfiltration",
                [
                    "This application reads details about the currently active data network",
                    "This application tries to find out if the currently active data network is metered"
                ]
            ],
            [
                "telephony_services_abuse",
                [
                    "This application makes phone calls"
                ]
            ],
            [
                "audio_video_eavesdropping",
                []
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address '' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/net/Proxy;-
>type()Ljava/net/Proxy$Type;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'timeout' on the 'N/A' port "
                ]
            ],
            [
                "PIM_data_leakage",
                []
            ],
            [
                "code_execution",
                [
                    "This application executes a UNIX command containing this argument: 'ps'",
                    "This application executes a UNIX command containing this argument: 'sh'"
                ]
            ]
        ]
```

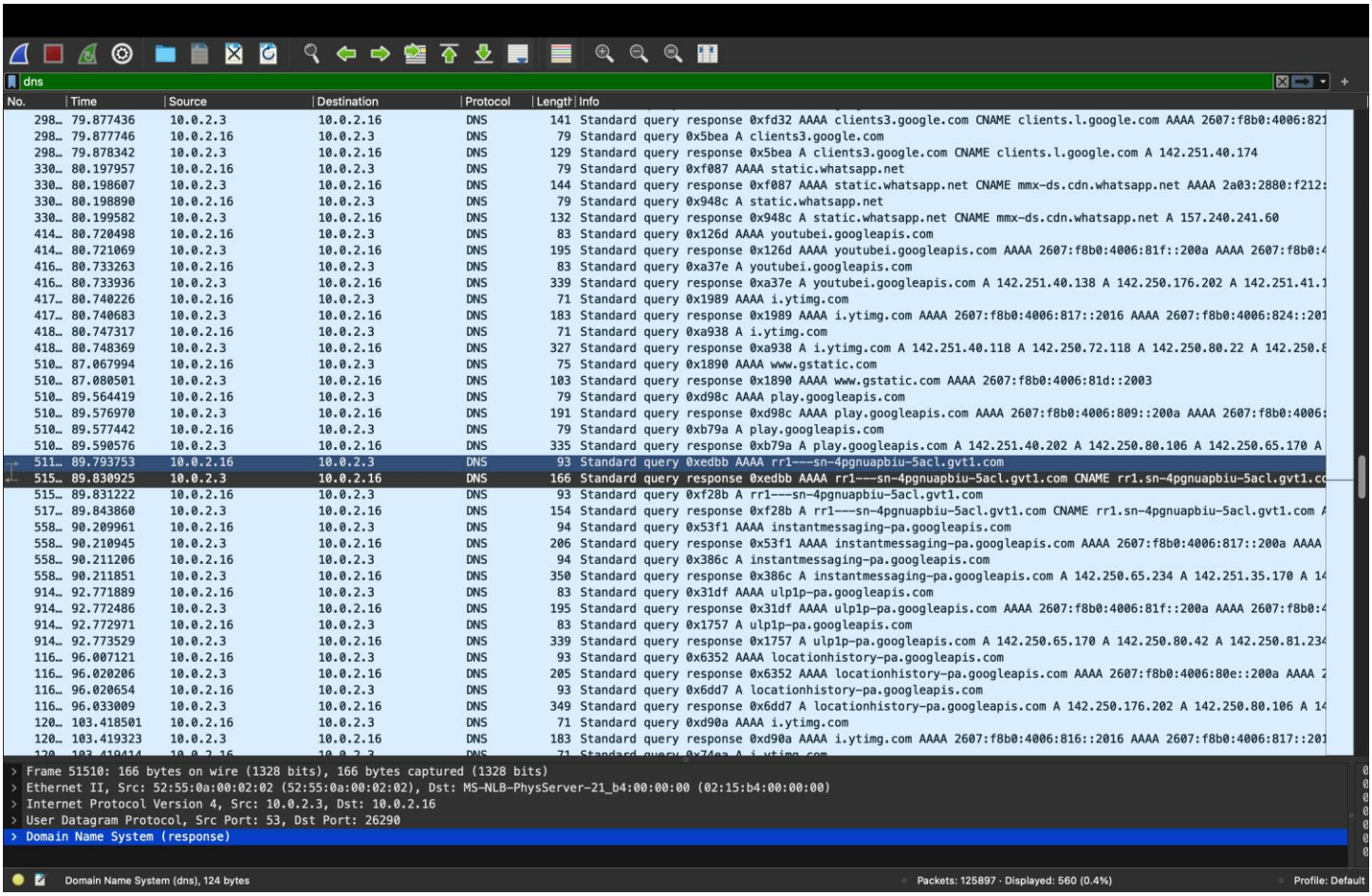
The application attempts to retrieve information about the active data network and ascertain whether it is metered, potentially infringing upon user privacy. Moreover, the application initiates phone calls without user consent, representing a significant misuse of telephony services. Additionally, it establishes suspicious connections to remote addresses through socket operations, which could indicate unauthorized network activity. Furthermore, the application executes UNIX commands such as 'ps' and 'sh', suggesting potential security vulnerabilities or malicious intent.


```
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.BLUETOOTH',\n 'android.permission.FOREGROUND_SERVICE',\n 'android.permission.GET_PACKAGE_SIZE',\n
'android.permission.GET_TASKS',\n 'android.permission.INSTALL_SHORTCUT',\n 'android.permission.INTERNET',\n
'android.permission.READ_EXTERNAL_STORAGE',\n 'android.permission.RECEIVE_BOOT_COMPLETED',\n
'android.permission.SYSTEM_ALERT_WINDOW',\n 'android.permission.UNINSTALL_SHORTCUT',\n 'android.permission.WAKE_LOCK',\n
'com.android.launcher.permission.INSTALL_SHORTCUT',\n 'com.android.launcher.permission.UNINSTALL_SHORTCUT',\n
'com.google.android.c2dm.permission.RECEIVE',\n 'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE']",
                    "Implied: []",
                    "Declared: []"
                ]
            ],
            [
                "features",
                [
                    "android.hardware.location.gps"
                ]
            ],
            [
                "libraries",
                [
                    "org.apache.http.legacy"
                ]
            ]
        ]
```

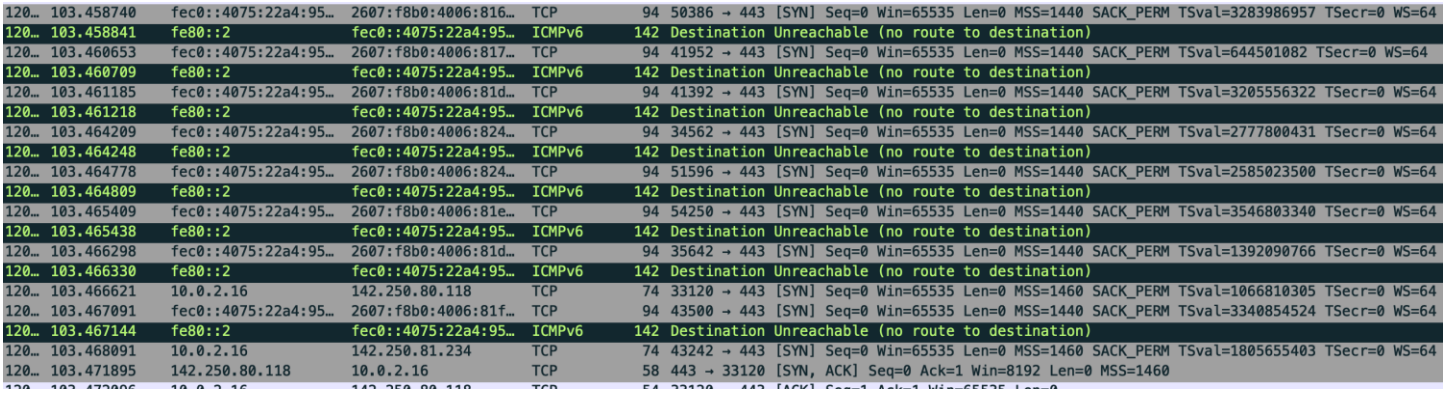

The permissions requested by the application cover a range of functionalities crucial for its operation and interaction with the device and network environment. These include accessing network and WiFi state to determine connectivity status, Bluetooth for wireless communication, and foreground service execution for running tasks in the foreground. Additionally, permissions like retrieving package size and tasks provide insights into the device's storage usage and running processes, while the ability to install and uninstall shortcuts facilitates user interface customization. The permission to access the internet enables the application to connect to remote servers, and reading external storage allows it to access files stored on the device. Furthermore, receiving boot completed broadcasts ensures that the application can start automatically after device boot-up, while the system alert window permission grants it the ability to display alerts on top of other apps. Acquiring wake locks helps prevent the device from sleeping while certain operations are ongoing. The application also utilizes the GPS feature for location-based functionalities. Moreover, it relies on the org.apache.http.legacy library for handling HTTP requests and responses. It's worth noting that no implied or declared permissions were identified, suggesting that the listed permissions are explicitly requested by the application without any additional implied permissions or declarations.

DYNAMIC ANALYSIS – WIRESHARK

Total Packets Traced : 125897 Packets
DNS Packets : 560 Packets
TCP Packets : 8771

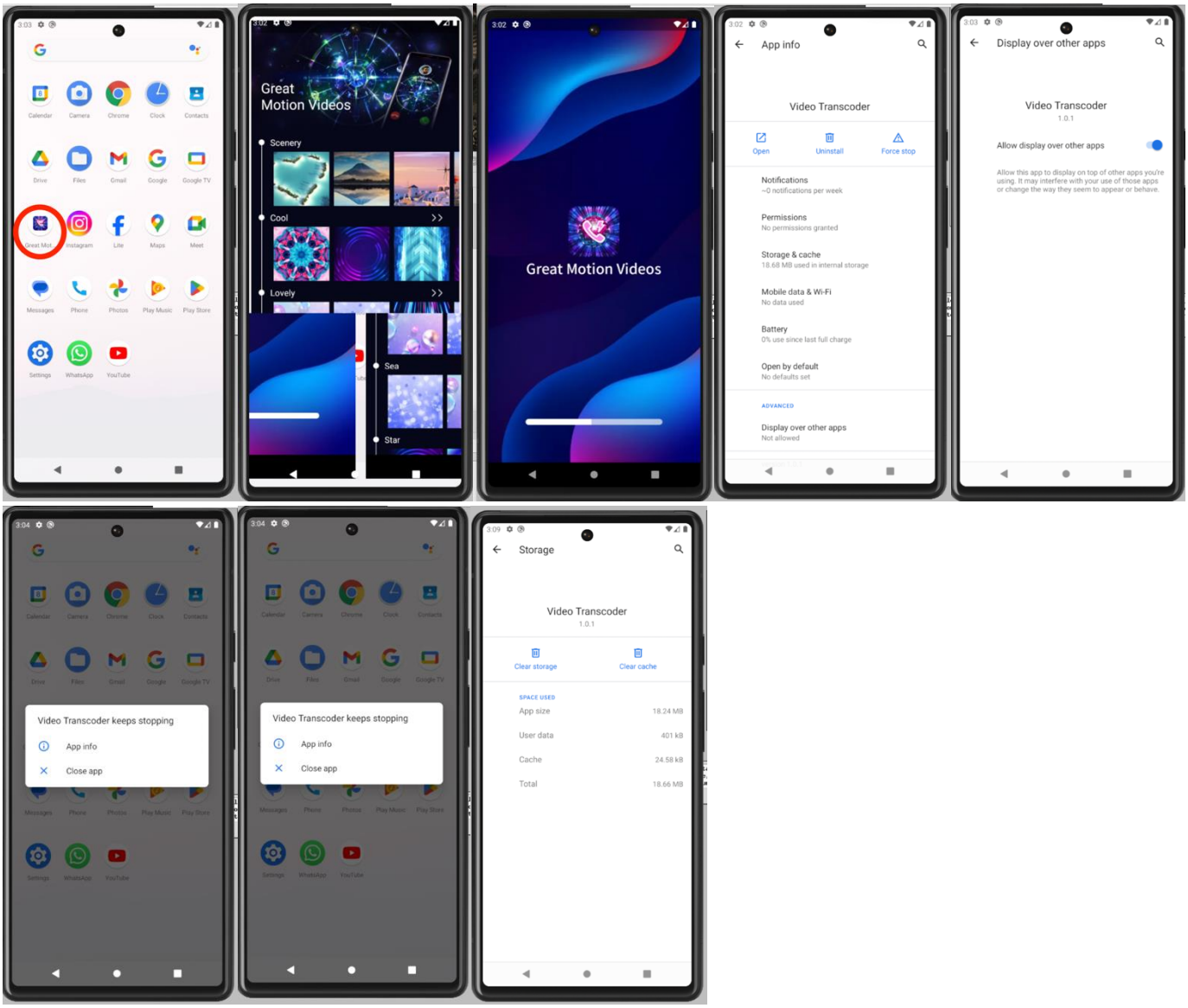


The application is observed to actively generate DNS queries specifically directed towards the URL rr1---sn-4pgnuapbiu-5acl.gvt1.com. This behavior raises concerns regarding the legitimacy and intentions of the website in question. Such activities may indicate attempts to establish connections with potentially unauthorized or malicious servers, warranting further investigation into the purpose and security implications of these actions.



The application has been observed sending ICMP (Internet Control Message Protocol) packets to an unreachable destination. This behavior is often indicative of network scanning or probing activities, suggesting potential attempts to explore or assess network vulnerabilities. Such actions could signify unauthorized or malicious behavior, raising concerns about the application's intentions and potential security risks associated with its network activities. Further analysis is recommended to investigate the nature and implications of these ICMP packet transmissions.

APPLICATION SCREENSHOTS



CONCLUSION

The application accesses the unique device ID, including the International Mobile Equipment Identity (IMEI) for GSM devices and the Mobile Equipment Identifier (MEID) or Electronic Serial Number (ESN) for CDMA phones. It has been observed that this unique device ID, specifically the IMEI and MEID, is being transmitted to an unreachable URL. To prevent potential security risks associated with the unauthorized transmission of sensitive device identifiers, it is advisable to implement measures to restrict or encrypt the transmission of such information. Additionally, conducting a thorough security assessment of the application's network activities and implementing appropriate data protection mechanisms can help mitigate the risk of unauthorized data exposure.

MALWARE APP 3 – UPS

STATIC ANALYSIS - ANDROWARN


```
        [
            "telephony_identifiers_leakage",
            [
                "This application reads the numeric name (MCC+MNC) of current registered operator",
                "This application reads the operator name"
            ]
        ],
```


The application reads the numeric name (MCC+MNC) of the current registered operator and the operator name raises concerns about potential privacy breaches and tracking capabilities. By accessing this information, the application could potentially track users' movements and behavior based on their network operator data.


```
        [
            "location_lookup",
            []
        ],
        [
            "connection_interfaces_exfiltration",
            [
                "This application reads details about the currently active data network"
            ]
        ],
        [
            "telephony_services_abuse",
            []
        ],
        [
            "audio_video_eavesdropping",
            [
                "This application records audio from the 'MIC' source ",
                "This application captures video from the 'CAMERA' source"
            ]
        ],
        [
            "suspicious_connection_establishment",
            []
        ],
        [
            "PIM_data_leakage",
            []
        ],
        [
            "code_execution",
            [
                "This application loads a native library"
            ]
        ]
```


The application's ability to record audio from the 'MIC' source and capture video from the 'CAMERA' source without explicit user consent poses significant privacy risks. Such functionalities could be exploited by malicious actors to eavesdrop on conversations, record sensitive information, or invade users' privacy without their knowledge. Additionally, the application's capability to load a native library raises concerns about potential code execution vulnerabilities, which could be exploited to execute arbitrary code on the device, leading to unauthorized access or control over the device's functionalities.

```
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.BLUETOOTH',\n 'android.permission.FOREGROUND_SERVICE',\n 'android.permission.GET_PACKAGE_SIZE',\n
'android.permission.GET_TASKS',\n 'android.permission.INSTALL_SHORTCUT',\n 'android.permission.INTERNET',\n
'android.permission.READ_EXTERNAL_STORAGE',\n 'android.permission.RECEIVE_BOOT_COMPLETED',\n
'android.permission.SYSTEM_ALERT_WINDOW',\n 'android.permission.UNINSTALL_SHORTCUT',\n 'android.permission.WAKE_LOCK',\n
'com.android.launcher.permission.INSTALL_SHORTCUT',\n 'com.android.launcher.permission.UNINSTALL_SHORTCUT',\n
'com.google.android.c2dm.permission.RECEIVE',\n 'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE']",
                    "Implied: []",
                    "Declared: []"
                ]
```

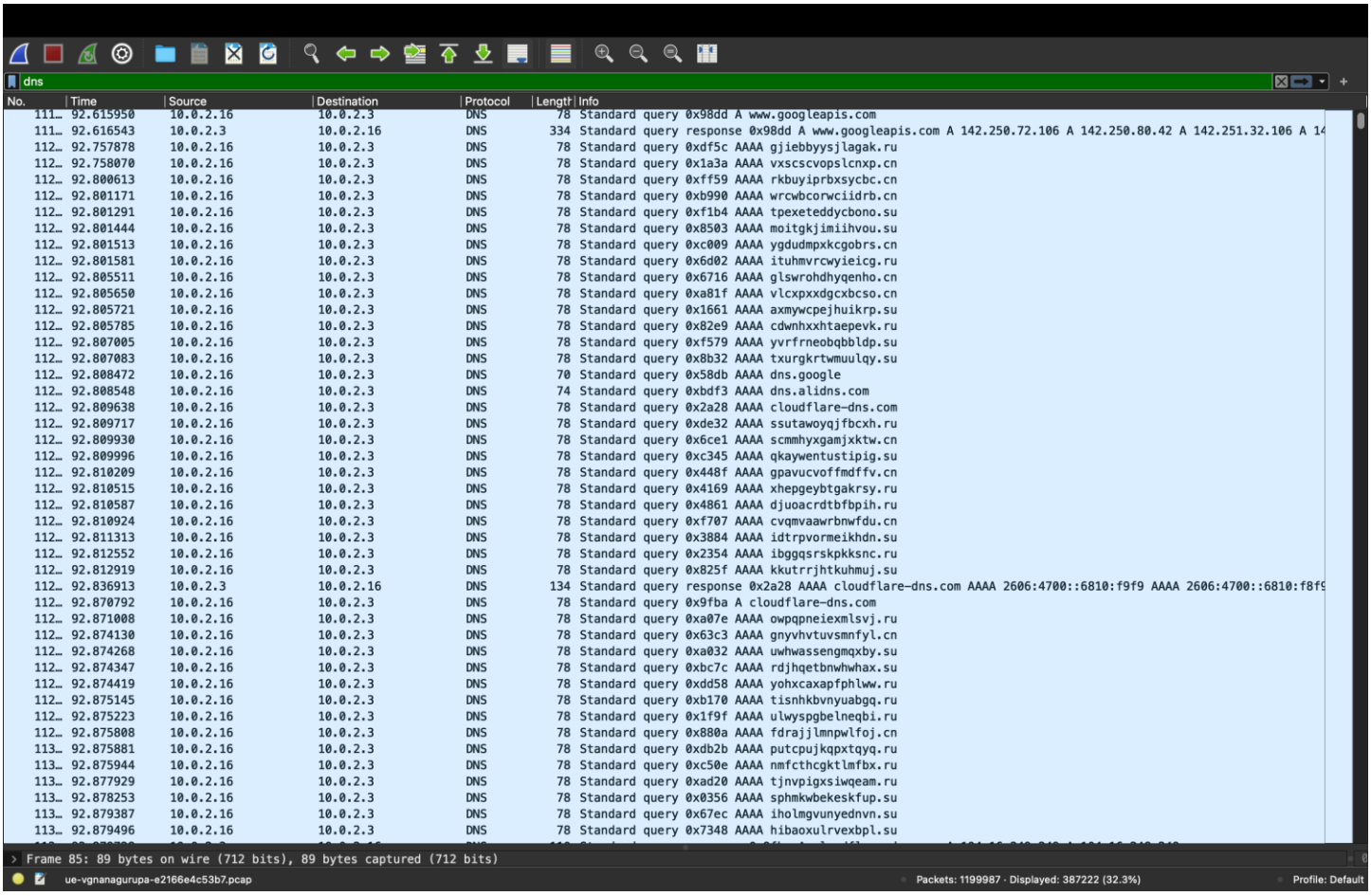

The requested permissions for this application primarily revolve around accessing network-related functionalities and system settings, with additional permissions related to handling shortcuts and receiving push notifications. Specifically, the app asks for permissions to access network state (ACCESS_NETWORK_STATE), WiFi state (ACCESS_WIFI_STATE), Bluetooth (BLUETOOTH), foreground services (FOREGROUND_SERVICE), internet connectivity (INTERNET), reading external storage (READ_EXTERNAL_STORAGE), receiving system boot completion events (RECEIVE_BOOT_COMPLETED), displaying system-level alerts (SYSTEM_ALERT_WINDOW), managing app shortcuts (INSTALL_SHORTCUT, UNINSTALL_SHORTCUT), and handling push notifications (com.google.android.c2dm.permission.RECEIVE, com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE). These permissions suggest that the application violates network connectivity for its functionality, as well as the ability to interact with system-level features like app shortcuts and push notifications.

DYNAMIC ANALYSIS – WIRESHARK ANALYSIS

Total number of Packets : 1199987

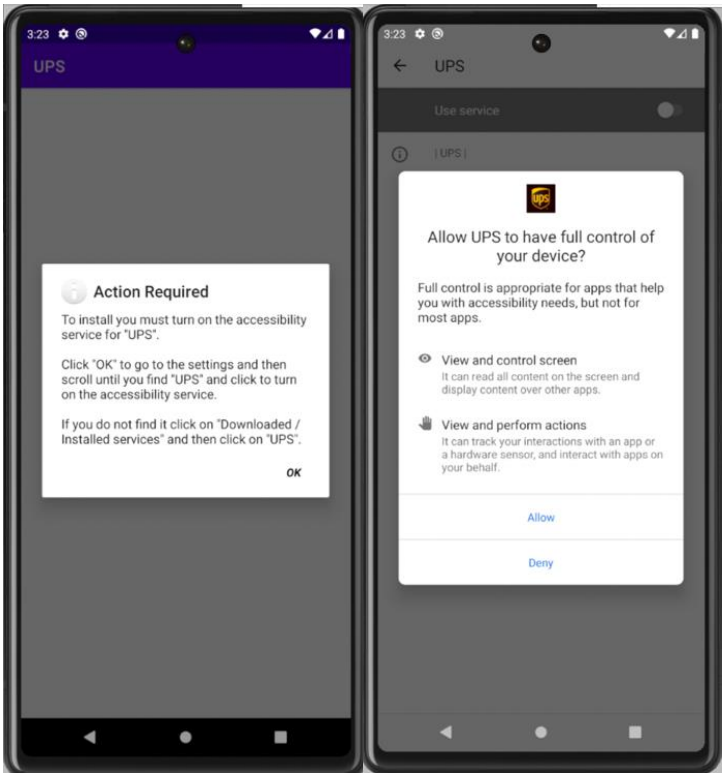
DNS Packets : 387222 Packets

TCP Packets : 1178257 Packets



The application is observed to generate DNS queries directed towards untrusted websites. This behavior raises concerns regarding potential security risks associated with accessing unreliable or suspicious domains. Such activity could expose the user to various threats, including malware distribution, phishing attacks, and unauthorized data access. To enhance security measures, it is recommended to monitor and restrict the application's DNS queries, implement robust domain filtering mechanisms, and employ network security protocols to prevent access to untrusted websites and mitigate the associated risks. Additionally, user education on safe browsing practices and the importance of avoiding interactions with suspicious domains can further enhance overall cybersecurity posture.

APPLICATION SCREENSHOTS



CONCLUSION

The application overrides the accessibility features and doesn't allow to change the accessibility settings. It is always running in the background. It doesn't allow to stop running/ force stop the application since it uses FOREGROUND_SERVICE and ACCESSIBILITY Permission to prevent from stop running the application.

In addition to its malicious behavior, the app requests permissions to view and control the screen, as well as to view and perform actions on behalf of the user. This capability allows the app to monitor and manipulate all content displayed on the screen, including interactions with other apps. By granting these permissions, users inadvertently provide the app with the ability to track their activities and execute actions without their explicit consent, posing serious privacy and security risks.

MALWARE APP 4 – VOICEMESSAGE

STATIC ANALYSIS - ANDROWARN


```
        "analysis_results": [
            [
                "telephony_identifiers_leakage",
                [
                    "This application reads the MCC+MNC of the provider of the SIM",
                    "This application reads the Service Provider Name (SPN)",
                    "This application reads the constant indicating the state of the device SIM card",
                    "This application reads the numeric name (MCC+MNC) of current registered operator",
                    "This application reads the operator name",
                    "This application reads the radio technology (network type) currently in use on the device for data
transmission"
                ]
            ],
```


The analysis results indicate that the application is potentially leaking telephony identifiers. It reads various sensitive information related to the mobile network and SIM card. Specifically, it accesses the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the SIM provider, the Service Provider Name (SPN), the state of the device SIM card, the numeric name of the current registered operator, the operator name, and the radio technology (network type) currently in use for data transmission. This information could potentially be used to track the user's location, monitor their network activity, or identify their mobile service provider, raising concerns about privacy and data security.


```
            [
                "location_lookup",
                []
            ],
            [
                "connection_interfaces_exfiltration",
                [
                    "This application reads details about the currently active data network"
                ]
            ],
            [
                "telephony_services_abuse",
                []
            ],
            [
                "audio_video_eavesdropping",
                []
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address '' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'connect, resolve' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/net/Proxy;-
>type()Ljava/net/Proxy$Type;' on the 'N/A' port "
                ]
            ],
            [
                "PIM_data_leakage",
                []
            ],
```


The analysis indicates several potential security risks associated with the application. While it doesn't engage in audio/video eavesdropping or abuse telephony services, it does involve suspicious connection establishment activities, such as opening sockets and connecting to remote addresses without clear purposes. Additionally, it reads details about the currently active data network, suggesting potential information leakage related to network activity. These activities could potentially compromise user privacy and expose sensitive data to unauthorized parties.

```
            [
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.CALL_PHONE',\n
'android.permission.FOREGROUND_SERVICE',\n 'android.permission.INTERNET',\n 'android.permission.KILL_BACKGROUND_PROCESSES',\n
'android.permission.QUERY_ALL_PACKAGES',\n 'android.permission.READ_CONTACTS',\n 'android.permission.READ_PHONE_STATE',\n
'android.permission.READ_SMS',\n 'android.permission.RECEIVE_SMS',\n 'android.permission.REQUEST_DELETE_PACKAGES',\n
'android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS',\n 'android.permission.SEND_SMS',\n 'android.permission.VIBRATE',\n
'android.permission.WAKE_LOCK',\n 'android.permission.WRITE_SMS']",
                    "Implied: []",
                    "Declared: []"
                ]
            ],
```

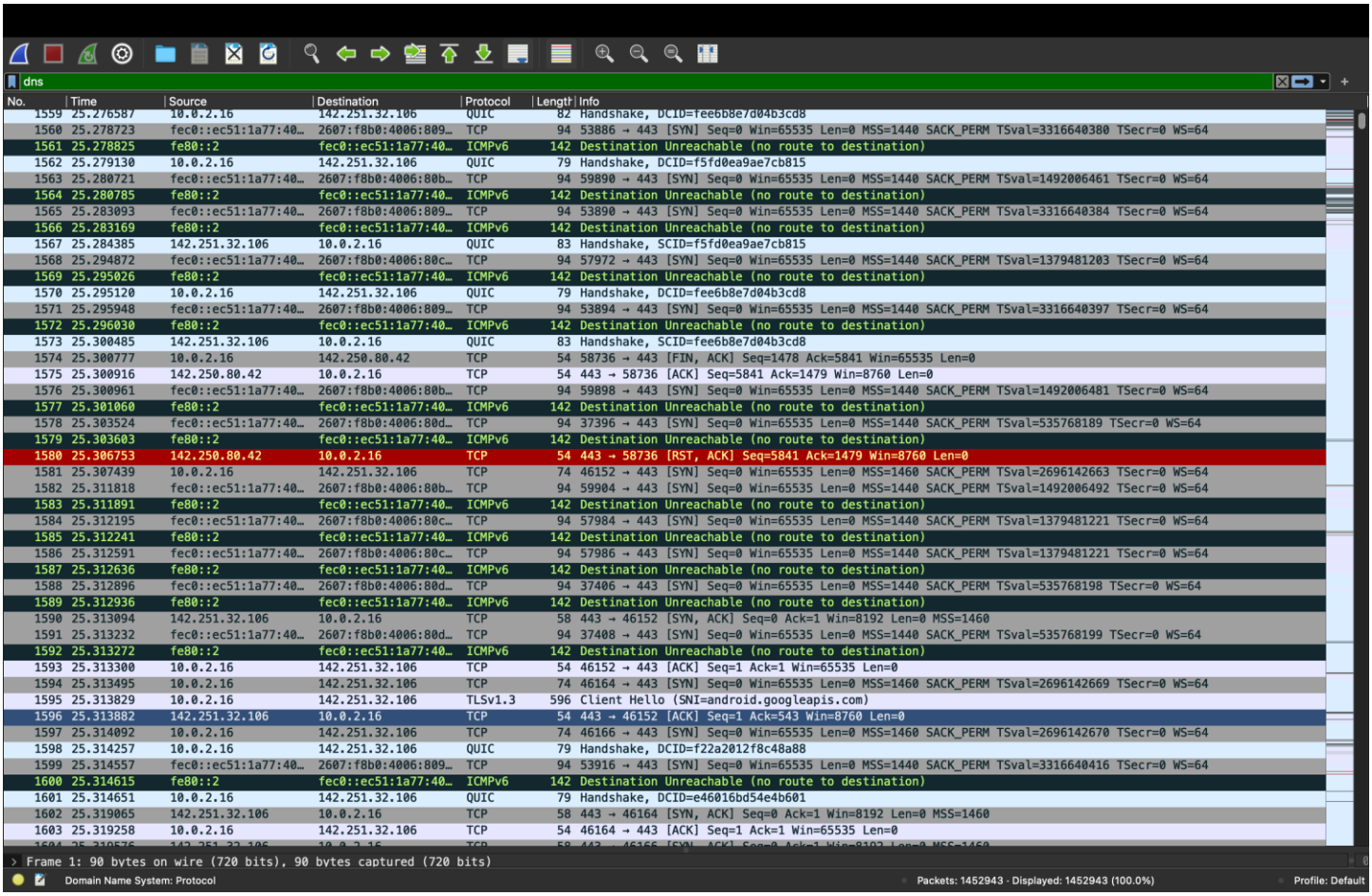

The permissions requested by the application reveal its broad access to various aspects of the device's functionality and user data. For instance, the "ACCESS_NETWORK_STATE" permission allows the app to monitor network connectivity, potentially enabling it to track a user's online activities. Additionally, the "CALL_PHONE" permission grants the ability to initiate phone calls without user intervention, which could lead to unauthorized call charges or privacy breaches. Similarly, permissions like "READ_SMS" and "SEND_SMS" provide access to the user's text messages, raising concerns about the confidentiality of communication. Moreover, the permission to "QUERY_ALL_PACKAGES" suggests that the app can gather information about installed applications on the device, possibly for targeted advertising or other purposes. Providing permissions like "KILL_BACKGROUND_PROCESS" and "FOREGROUND SERVICES" can introduce several risks to the security and performance of the device. These services may lead to increased battery drain, performance degradation, data loss, security vulnerabilities, user experience issues, privacy concerns, and resource hogging. Overall, while these permissions may be necessary for certain app functionalities, users should carefully consider the implications of granting such extensive access to their personal data and device features from a security standpoint.

DYNAMIC ANALYSIS – WIRESHARK

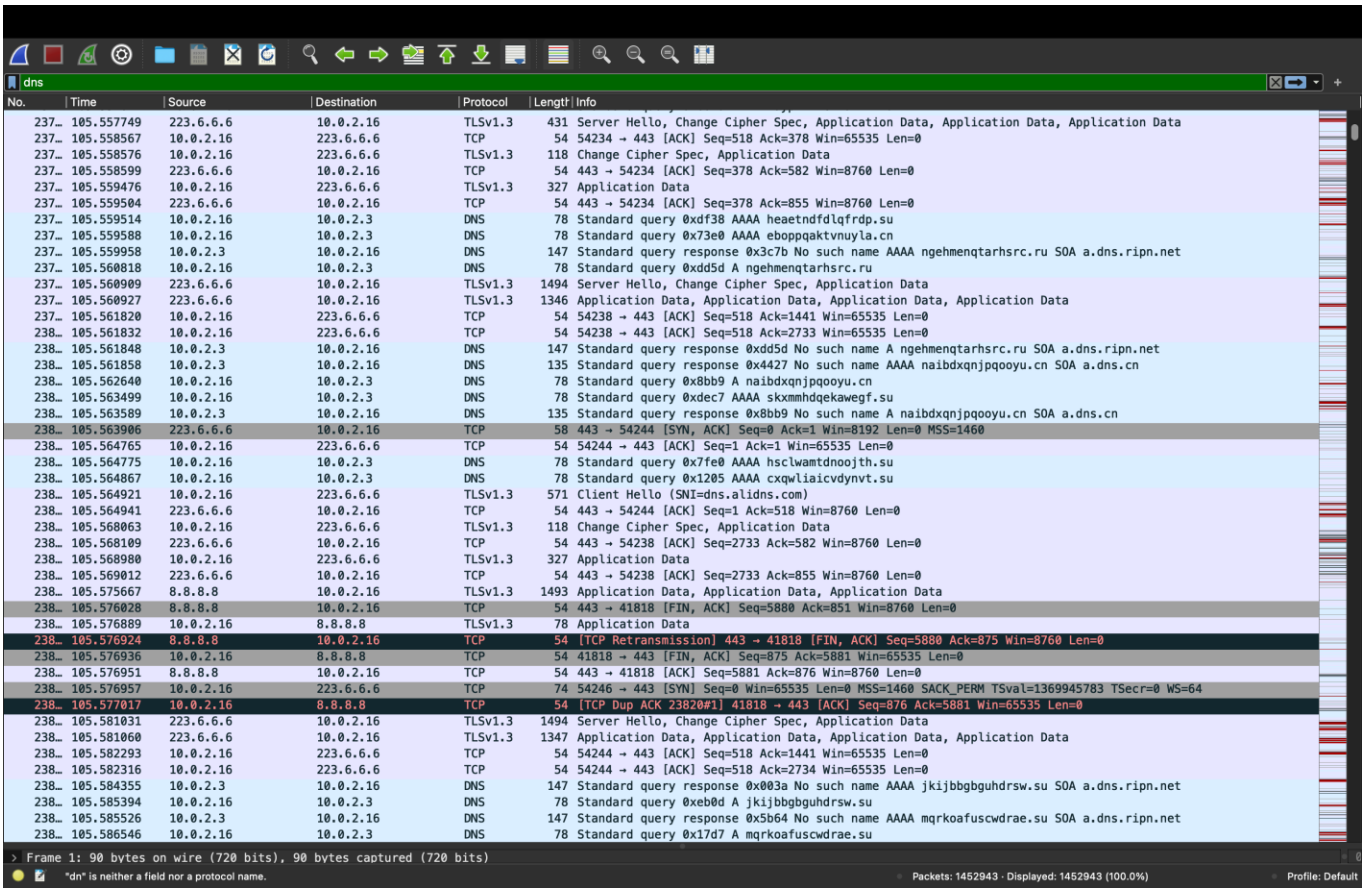
Total number of Packets : 1087942

DNS Packets : 752 Packets

TCP Packets :6317 Packets

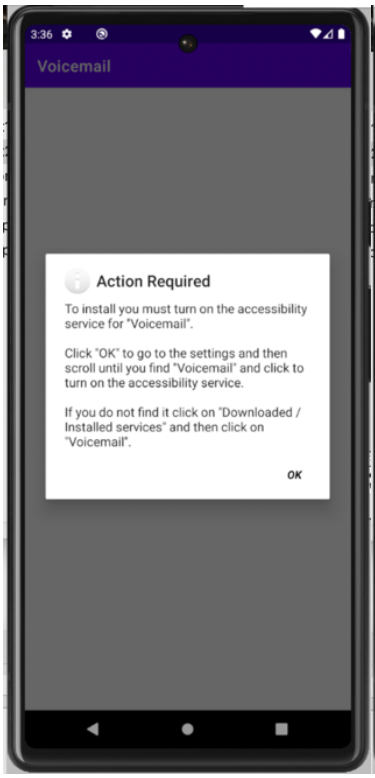


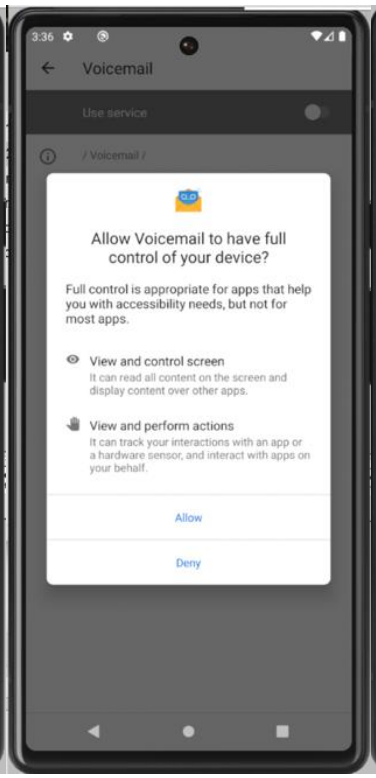
The application has been detected transmitting ICMP (Internet Control Message Protocol) packets to a destination that is unreachable. This behavior typically suggests network scanning or probing activities, indicating potential efforts to assess or explore network vulnerabilities. These actions may indicate unauthorized or malicious intent, prompting concerns regarding the application's motives and potential security implications related to its network behavior. Further investigation is advised to thoroughly examine the nature and consequences of these ICMP packet transmissions.

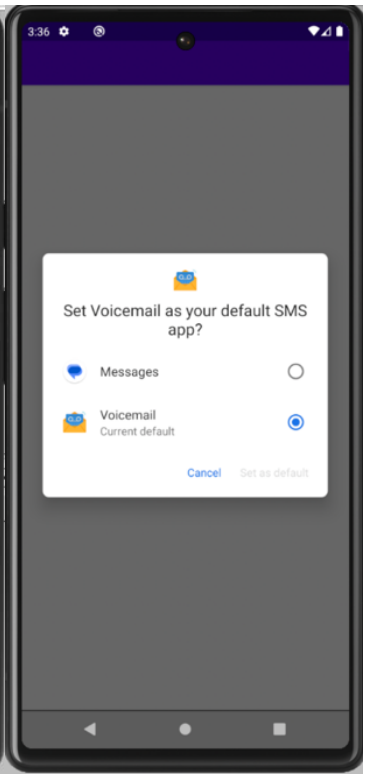


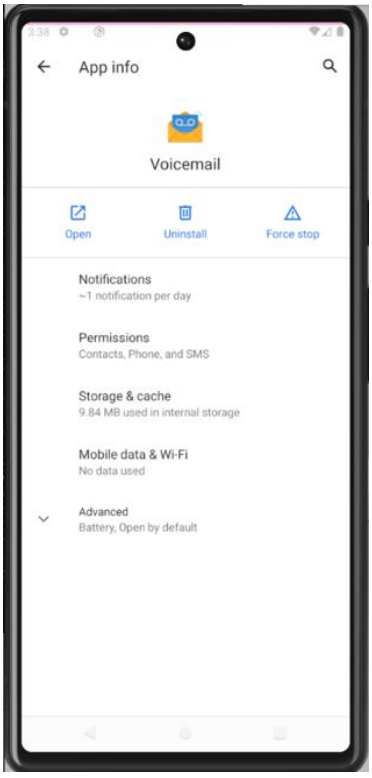
The application has been noted for initiating DNS queries aimed at untrustworthy websites. This action gives rise to apprehensions regarding the potential security hazards linked with accessing dubious or unreliable domains. Such behavior may expose users to a range of threats, including the distribution of malware, phishing attempts, and unauthorized access to data. To bolster security measures, it is advisable to monitor and restrict the application's DNS queries, implement robust domain filtering mechanisms, and deploy network security protocols to block access to untrusted websites and mitigate associated risks. Furthermore, educating users on safe browsing practices and emphasizing the importance of avoiding interactions with suspicious domains can further fortify overall cybersecurity defenses.

APPLICATION SCREENSHOTS









CONCLUSION

The application exhibits a concerning behavior whereby it overrides accessibility features and restricts users from modifying accessibility settings. It operates persistently in the background and prevents users from stopping or forcing the application to halt, leveraging FOREGROUND_SERVICE and ACCESSIBILITY permissions to maintain continuous operation. Moreover, alongside its malicious conduct, the app seeks permissions to view and control the screen, as well as to execute actions on behalf of the user. This functionality enables the app to monitor and manipulate all on-screen content, including interactions with other applications. By granting these permissions, users inadvertently grant the app access to track their activities and carry out actions without explicit consent, thereby introducing significant privacy and security vulnerabilities.

MALWARE APP 5 – FRUITNINJA

STATIC ANALYSIS - ANDROWARN


```
        "analysis_results": [
            [
                "telephony_identifiers_leakage",
                [
                    "This application reads the ISO country code equivalent for the SIM provider's country code",
                    "This application reads the MCC+MNC of the provider of the SIM",
                    "This application reads the Service Provider Name (SPN)",
                    "This application reads the constant indicating the state of the device SIM card",
                    "This application reads the current location of the device",
                    "This application reads the device phone type value",
                    "This application reads the numeric name (MCC+MNC) of current registered operator",
                    "This application reads the operator name",
                    "This application reads the radio technology (network type) currently in use on the device for data
transmission",
                    "This application reads the unique device ID, i.e the IMEI for GSM and the MEID or ESN for CDMA phones",
                    "This application reads the Cell ID value",
                    "This application reads the Location Area Code value"
                ]
            ],
```


This application exhibits concerning behavior related to telephony identifiers leakage, as it accesses a wide range of sensitive information associated with the user's mobile network and device. Specifically, it retrieves the ISO country code equivalent for the SIM provider's country code, the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the SIM provider, the Service Provider Name (SPN), and various identifiers such as the device's SIM card state, current location, phone type, registered operator, radio technology (network type), unique device ID (IMEI for GSM or MEID/ESN for CDMA phones), Cell ID, and Location Area Code. This extensive access to telephony-related data raises significant privacy and security concerns, as it could potentially be exploited for unauthorized tracking, profiling, or other malicious activities.

```
                "location_lookup",
                [
                    "This application reads location information from all available providers (WiFi, GPS etc.)"
                ]
            ],
            [
                "connection_interfaces_exfiltration",
                [
                    "This application reads details about the currently active data network",
                    "This application tries to find out if the currently active data network is metered"
                ]
            ],
            [
                "telephony_services_abuse",
                []
            ],
            [
                "audio_video_eavesdropping",
                []
            ],
            [
                "suspicious_connection_establishment",
                [
                    "This application opens a Socket and connects it to the remote address '' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'Ljava/net/Proxy;-
>type()Ljava/net/Proxy$Type;' on the 'N/A' port ",
                    "This application opens a Socket and connects it to the remote address 'timeout' on the 'N/A' port "
                ]
            ],
            [
                "PIM_data_leakage",
                []
            ],
            [
                "code_execution",
                [
                    "This application loads a native library: 'YandexMetricaNativeModule'",
                    "This application executes a UNIX command containing this argument: '1'",
                    "This application executes a UNIX command containing this argument: 'Ljava/lang/StringBuilder;-
>toString()Ljava/lang/String;'"
                ]
            ]
```


The analysis of this application further reveals several concerning behaviors related to data access and network activities. It reads location information from various providers, including WiFi and GPS, potentially compromising user privacy. Additionally, it accesses details about the active data network and attempts to determine if it is metered, suggesting potential monitoring or tracking capabilities. While no direct abuse of telephony services is identified, the application engages in suspicious connection establishment, opening sockets and connecting to remote addresses without clear purpose. Moreover, it exhibits capabilities for executing code, including loading a native library (YandexMetricaNativeModule) and executing UNIX commands, which could introduce security risks and facilitate unauthorized actions on the device. These findings underscore significant privacy and security concerns associated with the application's functionality and behavior.

```
                "permissions",
                [
                    "Asked: ['android.permission.ACCESS_NETWORK_STATE',\n 'android.permission.ACCESS_WIFI_STATE',\n
'android.permission.FOREGROUND_SERVICE',\n 'android.permission.GET_TASKS',\n 'android.permission.INTERNET',\n
'android.permission.QUICKBOOT_POWERON',\n 'android.permission.READ_APP_BADGE',\n 'android.permission.RECEIVE_BOOT_COMPLETED',\n
'android.permission.SEND_SMS',\n 'android.permission.SYSTEM_ALERT_WINDOW',\n 'android.permission.VIBRATE',\n
'android.permission.WAKE_LOCK',\n 'com.anddoes.launcher.permission.UPDATE_COUNT',\n
'com.google.android.c2dm.permission.RECEIVE',\n 'com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE',\n
'com.halfbrick.fruitninjafree.hack.permission.C2D_MESSAGE',\n 'com.htc.launcher.permission.READ_SETTINGS',\n
'com.htc.launcher.permission.UPDATE_SHORTCUT',\n 'com.huawei.android.launcher.permission.CHANGE_BADGE',\n
'com.huawei.android.launcher.permission.READ_SETTINGS',\n 'com.huawei.android.launcher.permission.WRITE_SETTINGS',\n
'com.majeur.launcher.permission.UPDATE_BADGE',\n 'com.oppo.launcher.permission.READ_SETTINGS',\n
'com.oppo.launcher.permission.WRITE_SETTINGS',\n 'com.sec.android.provider.badge.permission.READ',\n
'com.sec.android.provider.badge.permission.WRITE',\n 'com.sonyericsson.home.permission.BROADCAST_BADGE',\n
'com.sonymobile.home.permission.PROVIDER_INSERT_BADGE',\n 'me.everything.badger.permission.BADGE_COUNT_READ',\n
'me.everything.badger.permission.BADGE_COUNT_WRITE']",
                    "Implied: []",
                    "Declared: ['com.halfbrick.fruitninjafree.hack.permission.C2D_MESSAGE']"
                ]
```


The application's permissions grant it the ability to read SMS messages, which includes access to the content of incoming text messages. This capability enables the application to potentially extract sensitive information contained within SMS communications, such as authentication codes, one-time passwords, or personal messages. Additionally, the permission to send SMS messages allows the application to initiate outgoing text messages from the user's device. This functionality raises significant security concerns, particularly if the application is sending messages to premium-rate numbers without the user's knowledge or consent. Such actions could result in financial loss for the user, as premium-rate SMS messages often incur additional charges beyond standard messaging rates. Furthermore, unauthorized sending of SMS messages to premium numbers could indicate malicious behavior, such as fraud or unauthorized billing, highlighting the importance of vigilance when granting permissions to applications with access to SMS functionality.

DYNAMIC ANALYSIS – WIREHSARK

Total number of Packets : 1452943

DNS Packets : 2537Packets

TCP Packets : 128164 Packets

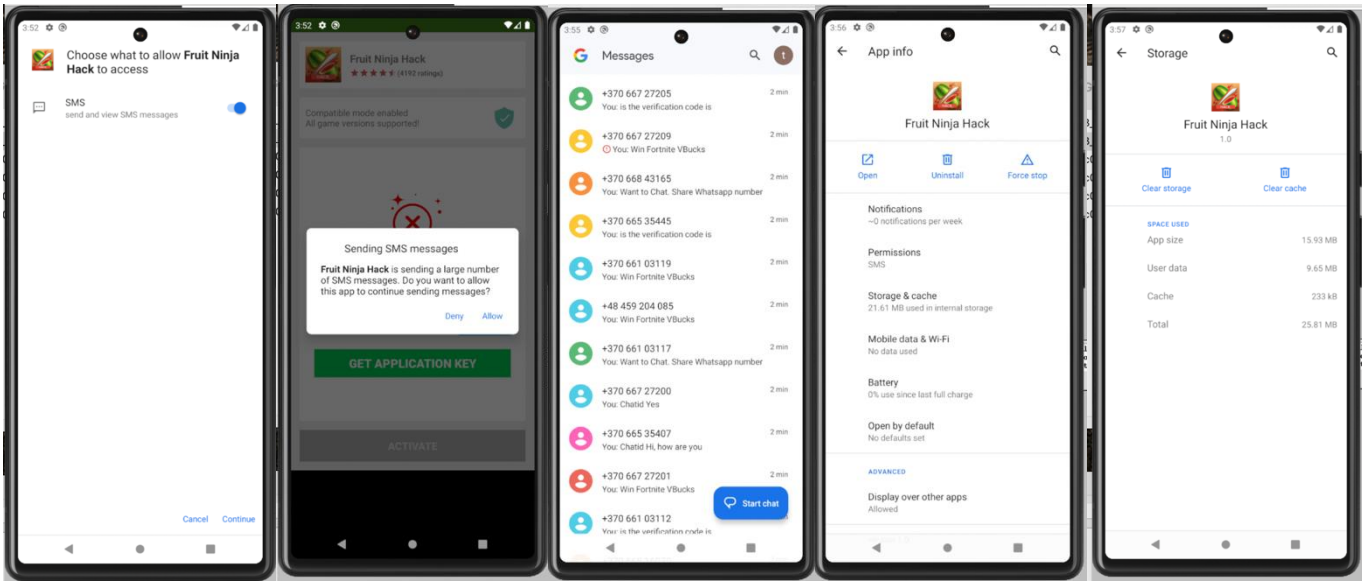
202…	162.630386	10.0.2.16	104.16.249.249	TCP	74	38476 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=2597423626 TSecr=0 WS=64
202…	162.630431	10.0.2.16	8.8.8.8	TLSv1.3	118	Change Cipher Spec, Application Data
202…	162.630443	8.8.8.8	10.0.2.16	TCP	54	443 → 54444 [ACK] Seq=219 Ack=628 Win=8760 Len=0
202…	162.630449	10.0.2.16	104.16.249.249	TCP	54	38470 → 443 [ACK] Seq=518 Ack=1441 Win=65535 Len=0
202…	162.630452	104.16.249.249	10.0.2.16	TLSv1.3	942	Application Data
202…	162.630472	10.0.2.16	104.16.249.249	TCP	54	38470 → 443 [ACK] Seq=518 Ack=2881 Win=65535 Len=0
202…	162.630475	10.0.2.16	10.0.2.3	DNS	78	Standard query 0xd1a0 A nrbgtbvmgmptdlu.cn
202…	162.630613	10.0.2.3	10.0.2.16	DNS	135	Standard query response 0xc7a2 No such name A pfrokhdaskmubvb.cn SOA a.dns.cn
202…	162.631288	223.5.5.5	10.0.2.16	TLSv1.3	760	Application Data, Application Data
202…	162.631957	10.0.2.16	104.16.249.249	TCP	54	38470 → 443 [ACK] Seq=518 Ack=3769 Win=65535 Len=0
202…	162.631964	10.0.2.16	104.16.249.249	TCP	74	38478 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=2597423627 TSecr=0 WS=64
202…	162.632020	10.0.2.16	8.8.8.8	TLSv1.3	323	Application Data
202…	162.632033	8.8.8.8	10.0.2.16	TCP	54	443 → 54444 [ACK] Seq=219 Ack=897 Win=8760 Len=0
202…	162.632042	10.0.2.16	10.0.2.3	DNS	78	Standard query 0x0c46 AAAA hfbfvohjojsdiuq.su
202…	162.632181	223.5.5.5	10.0.2.16	TCP	54	443 → 53476 [FIN, ACK] Seq=3439 Ack=855 Win=8760 Len=0
202…	162.632200	10.0.2.3	10.0.2.16	DNS	135	Standard query response 0xd1a0 No such name A nrbgtbvmgmptdlu.cn SOA a.dns.cn
202…	162.633864	10.0.2.16	8.8.8.8	TCP	74	54456 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM TSval=3346294247 TSecr=0 WS=64

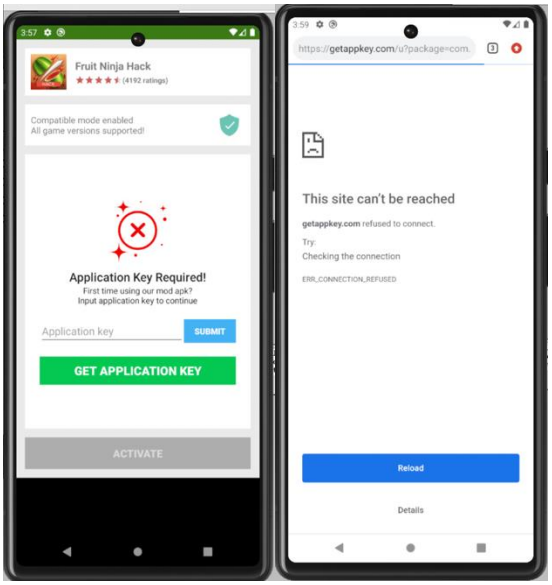
The application is detected generating DNS queries aimed at untrusted websites, prompting concerns about potential security threats linked to accessing unreliable or suspicious domains. This behavior poses risks such as malware distribution, phishing attacks, and unauthorized data access, exposing users to various dangers. To bolster security, it is advised to monitor and limit the application's DNS queries, establish robust domain filtering mechanisms, and deploy network security protocols to block access to untrusted websites and mitigate potential risks. Additionally, educating users on safe browsing practices and the significance of avoiding interactions with suspicious domains can bolster overall cybersecurity resilience.

```
676… 392.125989    10.0.2.16        142.251.40.202   ICMP      91 Destination unreachable (Port unreachable)
676… 392.425305    10.0.2.16        142.251.40.202   ICMP      91 Destination unreachable (Port unreachable)
676… 393.023294    10.0.2.16        142.251.40.202   ICMP      91 Destination unreachable (Port unreachable)
680… 394.222102    10.0.2.16        142.251.40.202   ICMP      91 Destination unreachable (Port unreachable)
687… 396.619497    10.0.2.16        142.251.40.202   ICMP      91 Destination unreachable (Port unreachable)
691… 398.365111    10.0.2.16        142.251.40.202   ICMP     136 Destination unreachable (Port unreachable)
967… 525.200948    10.0.2.16        10.0.2.3         ICMP     177 Destination unreachable (Port unreachable)
```

The application has been identified sending ICMP (Internet Control Message Protocol) packets to an unreachable destination. Such behavior often indicates network scanning or probing activities, hinting at potential attempts to assess or exploit network vulnerabilities. These actions raise concerns about the application's intentions and the security implications associated with its network behavior. It is recommended to conduct further investigation to fully understand the nature and impact of these ICMP packet transmissions.

APP SCREENSHOTS





CONCLUSION

The application flagrantly disregards user permissions by surreptitiously leveraging the user's device to dispatch SMS messages to premium numbers without explicit authorization, potentially leading to supplementary charges for the user. This unauthorized conduct is enabled by the permissions granted to the application, encompassing the capacity to peruse SMS messages, dispatch SMS messages, and execute background processes. Through the exploitation of these permissions, the application circumvents the user's control over their device, potentially culminating in unanticipated expenses and breaches of privacy. Such actions erode user confidence and engender substantial apprehensions regarding the application's integrity and adherence to ethical norms.