Date: 07/12/2024

MALWARE DETECTION AND AWARENESS REPORT

Malware Detection Analysis of Bilibili_1.31.0_.apk

1. OBJECTIVES

This report analyzes the security risks associated with the application *Bilibili_1.31.0_.apk*, flagged by one security vendor as potentially malicious by the use of VirusTotal for static analysis. The low detection rate (1/63) among antivirus vendors suggests limited immediate risk, but the presence of obfuscated code and advertising libraries calls for caution.

Bilibili is a Chinese online video-sharing platform that launched in 2009. It has become one of the most popular platforms in China, with over 326 million monthly active users and almost 4 billion daily video views – it is often referred to as the Chinese version of YouTube.

2. SUMMARY

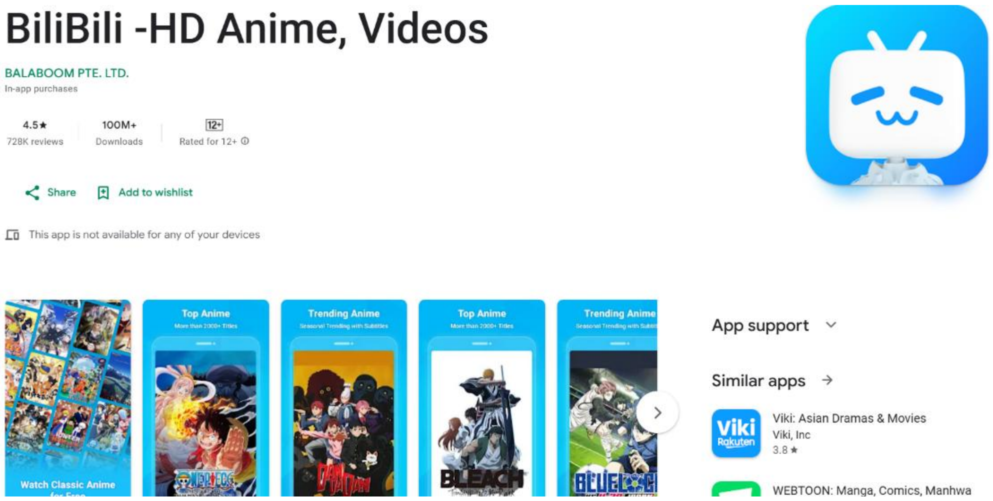
• Filename: Bilibili_1.31.0_.apk

• Size: 66.66 MB

• Detection Rate: 1/63 Security Vendors flagged it as malicious.

While most domains are hosted on reliable providers (e.g., Alibaba Cloud, Google APIs), the app's use of obfuscation and extensive permissions raises concerns about behavioral tracking and data collection

• Magic Information**:** Zip archive data, compression method=deflate.



BiliBili -HD Anime, Videos

BALABOOM PTE. LTD.

In-app purchases

4.5★ 728K reviews | 100M+ Downloads | 12+ Rated for 12+ ⓘ

This app is not available for any of your devices

App support

Similar apps

Viki: Asian Dramas & Movies
Viki, Inc
3.8★

WEBTOON: Manga, Comics, Manhwa

Fig. App Interface on Google Play Store

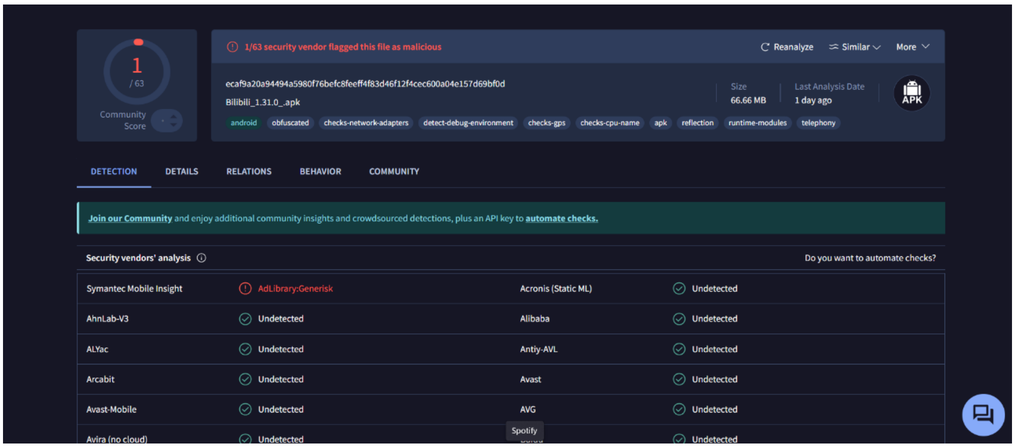
3. KEY FINDINGS

- **Flagged by Security Vendor:**

  Symantec Mobile Insight: Detected as *AdLibrary:Generisk*. This indicates the app may include a third-party advertising library that could potentially exhibit intrusive behaviors or track user activity without consent.

- **Not Detected by Other Vendors**

  62/63 antivirus engines, including industry leaders, did not flag the app as malicious. This indicates a low detection rate and reduces the likelihood of the app being a widespread threat.



1/63 security vendor flagged this file as malicious

ecaf9a20a94494a5980f76befc8feeff4f83d46f12f4cec600a04e157d69bf0d
Bilibili_1.31.0_.apk

Size 66.66 MB | Last Analysis Date 1 day ago

android | obfuscated | checks-network-adapters | detect-debug-environment | checks-gps | checks-cpu-name | apk | reflection | runtime-modules | telephony

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis — Do you want to automate checks?

Symantec Mobile Insight	AdLibrary:Generisk	Acronis (Static ML)	Undetected
AhnLab-V3	Undetected	Alibaba	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected
Avast-Mobile	Undetected	AVG	Undetected
Avira (no cloud)	Undetected		Undetected

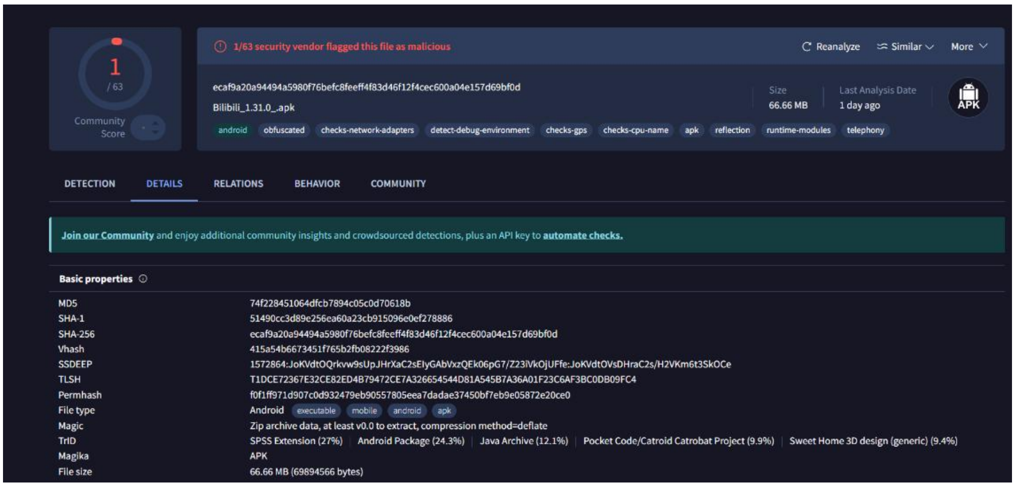
Fig. BiliBili APK Security Detection in VirusTotal

4. FILE PROPERTIES AND CHARACTERISTICS

File Type: Android APK (Executable for mobile devices)

MD5 Hash: 7af228451064dfcb7894c05c0d70618b

SHA-256 Hash: ecaf9a20a94494a5980f76befc8eeff4f83d46f12f4cec600a04e157d69bf0d



1/63 security vendor flagged this file as malicious

ecaf9a20a94494a5980f76befc8feeff4f83d46f12f4cec600a04e157d69bf0d
Bilibili_1.31.0_.apk

Size 66.66 MB | Last Analysis Date 1 day ago

android | obfuscated | checks-network-adapters | detect-debug-environment | checks-gps | checks-cpu-name | apk | reflection | runtime-modules | telephony

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Basic properties

MD5	74f228451064dfcb7894c05c0d70618b
SHA-1	51490cc3d89e256ea60a23cb915096e0ef278886
SHA-256	ecaf9a20a94494a5980f76befc8feeff4f83d46f12f4cec600a04e157d69bf0d
Vhash	415a54b6673451f765b2fb08222f3986
SSDEEP	1572864:JoKVdtOQrkvw9sUpJHrXaC2sElyGAbVxzQEk06pG7/Z23iVkOjUFfe:JoKVdtOVsDHraC2s/H2VKm6t3SkOCe
TLSH	T1DCE72367E32CE82ED4B79472CE7A326654544D81A545B7A36A01F23C6AF3BC0DB09FC4
Permhash	f0f1ff971d907c0d932479eb90557805eea7dadae37450bf7eb9e05872e20ce0
File type	Android executable mobile android apk
Magic	Zip archive data, at least v0.0 to extract, compression method=deflate
TrID	SPSS Extension (27%) | Android Package (24.3%) | Java Archive (12.1%) | Pocket Code/Catroid Catrobat Project (9.9%) | Sweet Home 3D design (generic) (9.4%)
Magika	APK
File size	66.66 MB (69894566 bytes)

Fig. BiliBili APK File Properties Analysis.

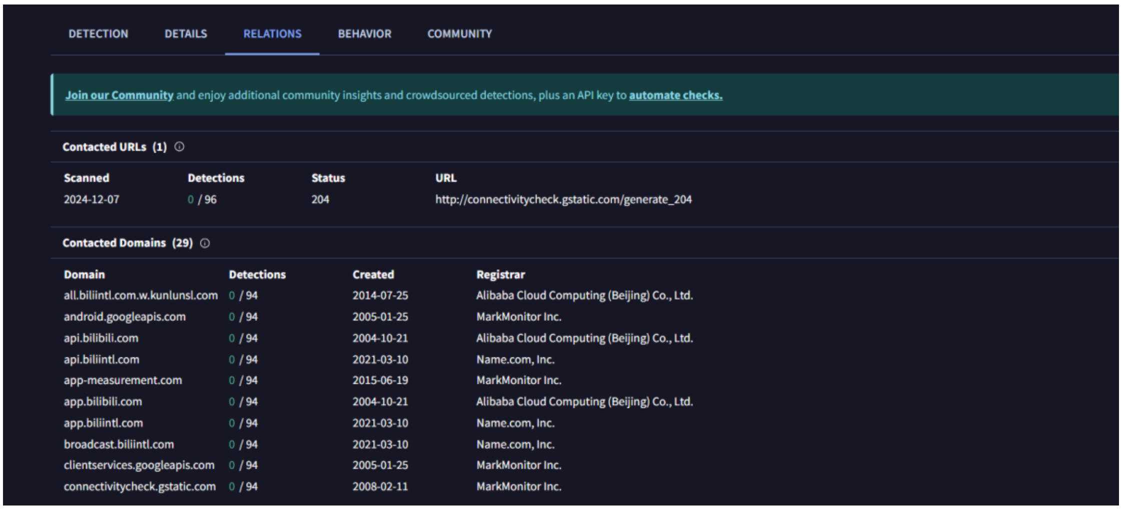
4.1 CHARACTERISTICS:

- **Obfuscated Code:** The application employs obfuscation, a technique used to obscure its code, making it difficult for researchers or antivirus tools to full analyze its behavior. While this is common for legitimate apps, it is also a hallmark of potentially malicious software.
- **Behavioral Features:** The app contains checks for:
  - **Network Adapters:** Could be used to track user connectivity or adjust functionality based on network conditions.
  - **GPS Location Data:** Indicates the app may request access to precise location information.
  - **Debug Environments:** May detect if it is running in an analysis tool or sandbox environment, suggesting it attempts to avoid detection.

5. CONTACTED URLS & DOMAINS

5.1 SCANNED URLS:

- Total: 1 URL scanned, with no detections.
- Example: http://connectivitycheck.gstatic.com/generate_204



Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Contacted URLs (1)

Scanned	Detections	Status	URL
2024-12-07	0 / 96	204	http://connectivitycheck.gstatic.com/generate_204

Contacted Domains (29)

Domain	Detections	Created	Registrar
all.biliintl.com.w.kunlunsl.com	0 / 94	2014-07-25	Alibaba Cloud Computing (Beijing) Co., Ltd.
android.googleapis.com	0 / 94	2005-01-25	MarkMonitor Inc.
api.bilibili.com	0 / 94	2004-10-21	Alibaba Cloud Computing (Beijing) Co., Ltd.
api.biliintl.com	0 / 94	2021-03-10	Name.com, Inc.
app-measurement.com	0 / 94	2015-06-19	MarkMonitor Inc.
app.bilibili.com	0 / 94	2004-10-21	Alibaba Cloud Computing (Beijing) Co., Ltd.
app.biliintl.com	0 / 94	2021-03-10	Name.com, Inc.
broadcast.biliintl.com	0 / 94	2021-03-10	Name.com, Inc.
clientservices.googleapis.com	0 / 94	2005-01-25	MarkMonitor Inc.
connectivitycheck.gstatic.com	0 / 94	2008-02-11	MarkMonitor Inc.

Fig. BiliBili APK Relations Overview

5.2 CONTACTED DOMAINS:

The app communicated with **29 domains** during its activity. While most domains are hosted by reputable providers, the number of connections raises concerns about potential behavioral tracking or unauthorized data transfers.

Examples of Domains Contacted:

- **api.bilibili.com** – Core API for app functionality.
- **app.bilibiliintl.com** – Supports app operations for international users.

➢ **android.googleapis.com** – Trusted Google service endpoint.

5.3 DOMAIN HOSTING PROVIDERS:

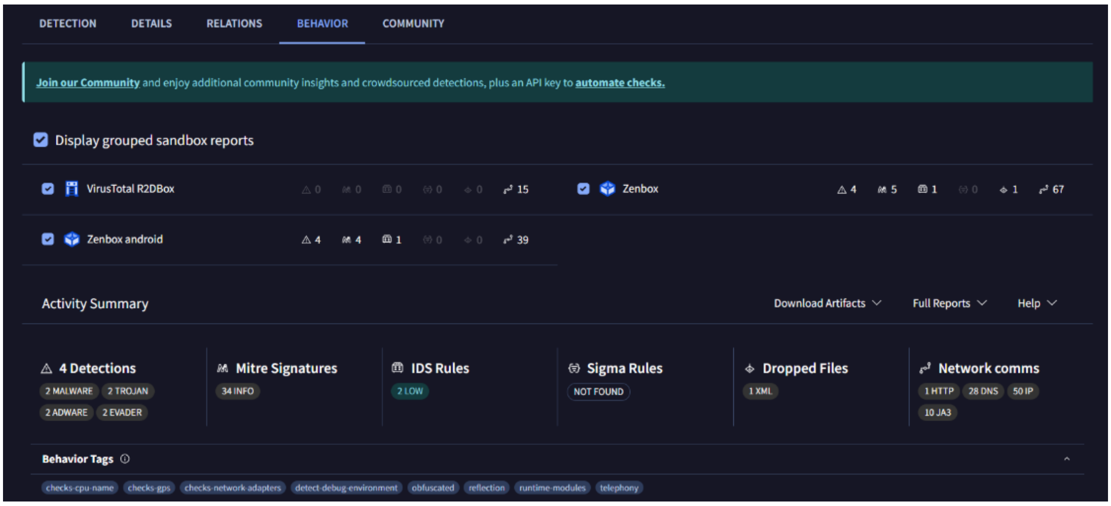
Reliable providers include **Alibaba Cloud Computing** and **Google APIs**, which show no direct evidence of malicious behavior.

6. BEHAVIORAL ANALYSIS

6.1 DYNAMIC ANALYSIS DETECTION

Dynamic analysis means the app's behavior was tested in a controlled environment (sandbox). Two sandbox tools flagged it as **malicious**:

- **VirusTotal R2DBox** did not detect any specific malicious behavior.
- **Zenbox Android** flagged the app with the following malicious tags:
  - ○ **Malware**: Indicates the app contains harmful code designed to harm devices or steal information.
  - ○ **Trojan**: A Trojan disguises itself as legitimate software while performing malicious activities in the background.
  - ○ **Adware**: The app may push intrusive advertisements, sometimes redirecting users to unsafe or malicious websites.
  - ○ **Evader**: Indicates the app uses techniques to avoid detection by antivirus software or security systems.



Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

☑ Display grouped sandbox reports

☑ VirusTotal R2DBox 0 0 0 0 0 15

☑ Zenbox 4 5 1 0 1 67

☑ Zenbox android 4 4 1 0 0 39

Activity Summary

4 Detections: 2 MALWARE, 2 TROJAN, 2 ADWARE, 2 EVADER

Mitre Signatures: 34 INFO

IDS Rules: 2 LOW

Sigma Rules: NOT FOUND

Dropped Files: 1 XML

Network comms: 1 HTTP, 28 DNS, 50 IP, 10 JA3

Behavior Tags: checks-cpu-name, checks-gps, checks-network-adapters, detect-debug-environment, obfuscated, reflection, runtime-modules, telephony

Fig. BiliBili APK Security Behavior Analysis

6.2 MITRE ATT&CK TECHNIQUES

The app uses techniques that map to common tactics used by cybercriminals. These include:

i. **Discovery (TA0007):** The app collects system information such as hardware details, network adapters, or GPS location. This data could be used for profiling the victim or for targeting attacks.

ii. **Command and Control (C2) (TA0011):** The app establishes communication with external servers (as seen in the network logs). This allows attackers to:

- Exfiltrate sensitive data (e.g., location, personal files).
- Receive commands to execute further malicious actions (e.g., stealing more data or installing more malware).

iii. **Defense Evasion (TA0030):** The app employs methods to bypass detection, such as:

- Obfuscating its code to make it hard for security tools to analyze.
- Detecting if it’s running in a debugging or analysis environment and altering behavior accordingly.

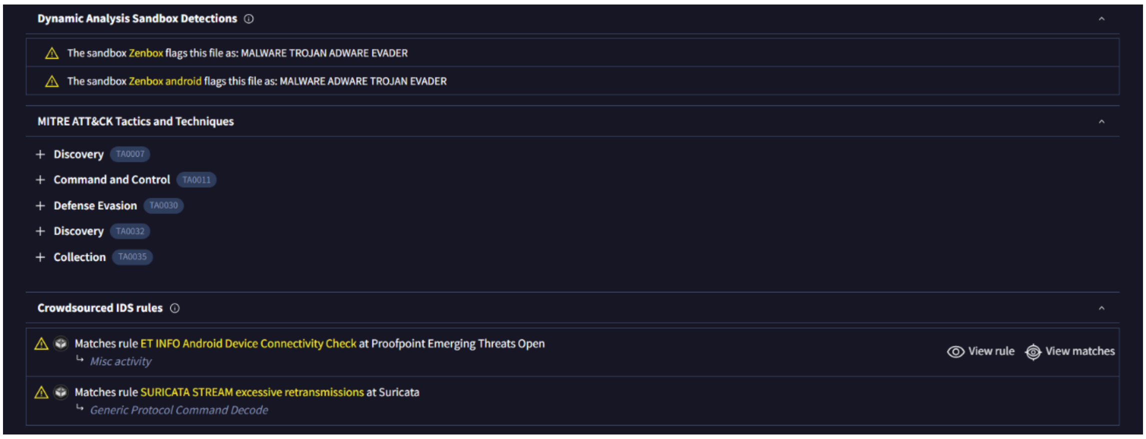
iv. **Collection (TA0035):** The app collects sensitive user data, potentially including messages, contacts, or device analytics.

6.3 IDS RULES MATCHED

Intrusion Detection System (IDS) rules are used to identify suspicious activity. Two rules were triggered:

i. **ET INFO Android Device Connectivity Check:** Indicates the app is performing unexpected connectivity checks. This could mean the app is verifying internet availability before contacting its command server.

ii. **SURICATA STREAM excessive retransmissions:** Suggests suspicious or abnormal network activity, such as excessive retries to communicate with external servers. This could point to the app’s efforts to maintain a stable connection to its malicious infrastructure.



Dynamic Analysis Sandbox Detections

⚠ The sandbox Zenbox flags this file as: MALWARE TROJAN ADWARE EVADER

⚠ The sandbox Zenbox android flags this file as: MALWARE ADWARE TROJAN EVADER

MITRE ATT&CK Tactics and Techniques

+ Discovery TA0007
+ Command and Control TA0011
+ Defense Evasion TA0030
+ Discovery TA0032
+ Collection TA0035

Crowdsourced IDS rules

⚠ Matches rule ET INFO Android Device Connectivity Check at Proofpoint Emerging Threats Open
↳ *Misc activity*

⚠ Matches rule SURICATA STREAM excessive retransmissions at Suricata
↳ *Generic Protocol Command Decode*

Fig. Detailed Dynamic Analysis showing MITRE ATT&CK Tactics and IDS Rules

6.4 NETWORK COMMUNICATION

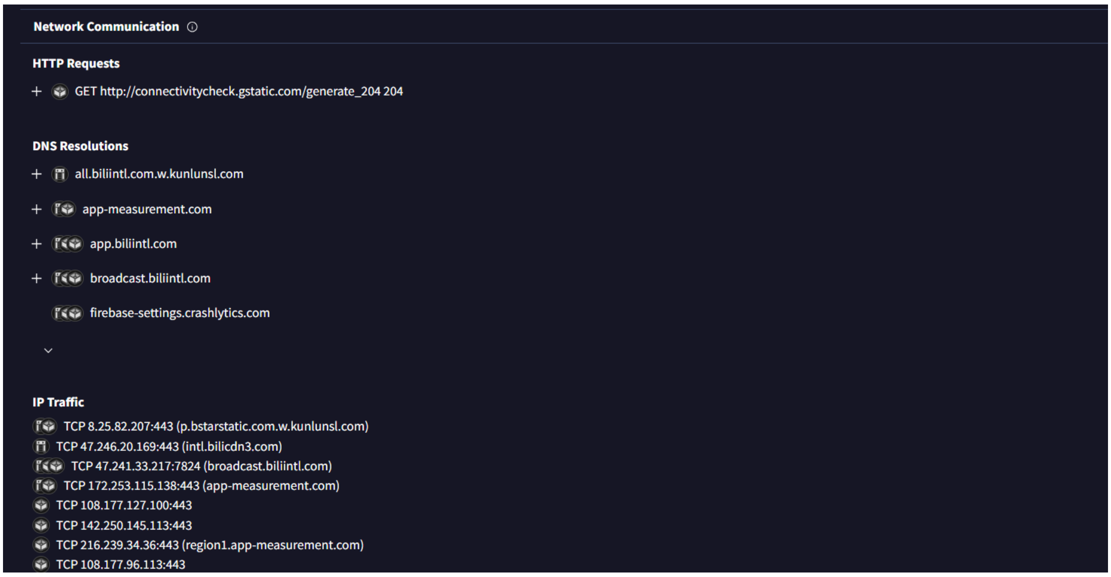
The app’s network behavior is one of the strongest indicators of its malicious intent:

i. **HTTP Request:** The app sends a GET request to `http://connectivitycheck.gstatic.com/generate_204`. This is a legitimate domain often used to check internet connectivity; however, the app's use of this may be to test connectivity before malicious activity.

ii. **DNS Resolutions:** The app resolves multiple domains:

- `app.biliintl.com`, `broadcast.biliintl.com`: These domains could be used for data collection or exfiltration.
- `app-measurement.com`, `firebase-settings.crashlytics.com`: These are typically associated with analytics but may have been exploited here.

iii. **IP Traffic:** The app communicates with several external IP addresses. These IPs might belong to command-and-control servers or platforms used to steal or manipulate data.



```
Network Communication ⓘ

HTTP Requests
+ GET http://connectivitycheck.gstatic.com/generate_204 204

DNS Resolutions
+ all.biliintl.com.w.kunlunsl.com
+ app-measurement.com
+ app.biliintl.com
+ broadcast.biliintl.com
  firebase-settings.crashlytics.com

IP Traffic
TCP 8.25.82.207:443 (p.bstarstatic.com.w.kunlunsl.com)
TCP 47.246.20.169:443 (intl.bilicdn3.com)
TCP 47.241.33.217:7824 (broadcast.biliintl.com)
TCP 172.253.115.138:443 (app-measurement.com)
TCP 108.177.127.100:443
TCP 142.250.145.113:443
TCP 216.239.34.36:443 (region1.app-measurement.com)
TCP 108.177.96.113:443
```

Fig. Network Communications

6.5 BEHAVIORAL INDICATORS

The app's observed behaviors provide further evidence of its malicious purpose:

- **System Checks:** It gathers information such as CPU details, GPS location, and network adapter data to build a profile of your device.
- **Debug Environment Detection:** The app can detect if it's being analyzed (e.g., in a sandbox) and may behave differently to evade detection.
- **Obfuscation:** The app's code is deliberately hidden or scrambled, making it harder for analysts to understand its purpose.
- **Telephony Access:** The app may interact with telephony features (e.g., SMS, call logs), potentially for data theft or to execute further attacks.

7. OBSERVATION AND ANALYSIS

- **Detection by Symantec Mobile Insight:** The only vendor that flagged the file highlighted an issue with an advertising library, categorizing it as "AdLibrary:Generisk." This often points to potentially unwanted behaviors such as invasive ads or tracking.
- **Obfuscation Indicators:** Tags such as "Obfuscated" and "Reflection" suggest that the file employs techniques to make its code harder to analyze, potentially hiding malicious functions. The presence of "Detect-debug-environment" implies anti-analysis mechanisms to thwart security researchers or malware analysts.
- **Network Monitoring:** Contacted URLs and domains are associated with well-known services (e.g., Google APIs, Alibaba Cloud), which may indicate legitimate functionalities. However, these connections should be monitored further for unusual behaviour.
- **Excessive permissions:** The app likely requests excessive permissions based on its behavioral features. These permissions may include access to GPS or location data, network configuration and adapter information, and system debugging settings. Access to GPS or location data allows an app to track the user's real-time location. If not essential for the app’s functionality (e.g., navigation or location-based services), this can pose significant privacy risks, as it exposes sensitive user information.
- **File Attributes:** The mix of packaging indicators (e.g., Java Archive, SPSS Extension) may signal a multi-purpose or hybrid application, which could be exploited maliciously if not appropriately designed.

8. MITIGATION STEPS

8.1 IMMEDIATE STEPS

- **Uninstall the App Immediately:** Go to your device settings, locate the app, and uninstall it.
- **Revoke Permissions:** Revoke permissions granted to the app (e.g., access to GPS, contacts, or SMS).
- **Disconnect from Networks:** Turn off Wi-Fi and mobile data temporarily to stop any ongoing malicious communication.
- **Scan Your Device:** Use a trusted antivirus or security application to perform a thorough scan of your device.

8.2 PREVENTION TIPS

- **Download Only from Trusted Sources:** Stick to official app stores and verify app developers.
- **Review App Permissions:** Avoid granting excessive permissions, especially for apps that don’t need them.

- **Enable Security Features:** Enable real-time protection on your device and keep your software updated.

9. RECOMMENDATION

- **Avoid Installation:** Refrain from installing the application until its legitimacy is verified by deeper analysis.
- **Perform Dynamic Analysis:** Use a secure sandbox environment to run the APK and monitor its runtime behavior, including file creation, registry modifications, and additional network communications.
- **Network Inspection:** Examine the traffic generated by the application to detect any unauthorized data exfiltration or connections to untrusted servers.
- **Update Security Software:** Ensure your device's antivirus and security software are up-to-date for protection against potential threats.
- **Vendor Contact:** If the application is critical for usage, reach out to the developers or the hosting platform to verify its authenticity.

10. CONCLUSION

The analysis of the Bilibili_1.31.0_.apk application highlights the importance of maintaining vigilance and awareness regarding mobile app installations. While the low detection rate by antivirus vendors might suggest minimal immediate risk, the presence of obfuscated code, advertising libraries, and intrusive behaviors warrants concern. Obfuscation, excessive permissions, and communication with multiple domains pose potential privacy and security risks, emphasizing the need for proactive measures. Users should prioritize downloading apps only from trusted sources, carefully reviewing requested permissions, and enabling robust security features on their devices. Additionally, organizations and individuals must adopt advanced security practices, such as dynamic sandboxing and network traffic analysis, to identify and mitigate threats effectively.

Awareness plays a critical role in combating potential cybersecurity threats. Educating users about the implications of installing apps with excessive permissions or unknown behaviors is crucial. Regular updates to antivirus software and thorough scrutiny of app developers can further safeguard against risks. While the analyzed application is not flagged as a widespread threat, its features and behavior indicate the necessity for caution. By fostering awareness and adhering to best practices in cybersecurity, users can better protect their data and devices from potential exploitation.