Journal of Applied Engineering, Technology and Management (JAETM)

FORENSIC AND BEHAVIOR ANALYSIS OF FREE ANDROID VPNS

Tashi Wangchuk[1], Digvijaysingh Rathod[2]
Department of Information Technology, Jigme Namgyel Engineering College, Dewathang, Bhutan[1]
Institute of Forensic Science, Gujarat Forensic Sciences University, Gandhinagar, Gujarat, India[2]
tashiwangchuk@jnec.edu.bt[1] , digvijay.rathod@gfsu.edu.in[2]

Abstract - Millions of users worldwide use VPN clients to either circumvent censorship or to access geo-blocked content, and specifically for privacy and security purposes. In the pretext of secured communication and privacy, numerous free android-based VPNs are being pushed up in the Google Play store. However, the users aren't sure or aware of whether the VPN is truly secure or just leaking their data. So, the forensic and behavior analysis of selected free android VPNs was carried out to study the usability of free android-based VPNs in terms of providing security and privacy; specifically, the presence of dangerous permissions, malware presence, traffic encryption, the DNS leaks, and the possibility of leaving forensic artifacts on the device after the VPN use. The study revealed considerable portion of the sample free VPNs were flagged malicious and had dangerous levels of permissions in use. While some failed the DNS leak test and some VPNs even did not encrypt the traffic. Given the availability of a huge number of Free VPNs in the Google Play store, it was found important that the users must be aware of the inherent risks put by the use of these Free VPNs.

Keywords— Android Permissions, Android VPN, Behavior, Forensic analysis

I. INTRODUCTION

Digital forensics is a branch of forensic science focusing on the recovery and investigation of raw data residing in electronic or digital devices. Mobile forensics is a branch of digital forensics related to the recovery of digital evidence [1]. Smartphones are being used by individuals for performing a multitude of activities such as browsing the internet, accessing online banking services and performing transactions, storing their private data, and so on. The Android applications in the phone facilitate the users with many attractive features and make the user's life easy. According to Brandom [2], after ten years of launch, there are 2.5 billion active Android devices. Since the introduction of Android by Google, the market share of Android had reached 76% as compared to 22% of Apple's iOS [3].

In 2019, Ivar has mentioned that when the keyword VPN was searched in the Google Play store, over 250 apps get listed and not all of them are worthy of downloading and installing on our devices. When 50 apps were studied, it was found that a huge number of VPN apps for Android had questionable developers who had no information other than the mail address and their privacy policy was not proper [4].

The function of the VPN is to sufficiently hide the online activity of the users from the Internet Service Provider (ISP) and others thereby preventing the personal information from getting into the others' hands. So, censorship circumvention, gaining anonymity while online, and protection from monitoring and tracking are the main reasons which the VPN user desires. Roach [5] in his article states that the purpose of VPNs is to protect the user from intrusive persons and agencies, such as ISP and the Government.
There are many countries in which VPN usage is regulated and the VPN services are blocked in different ways. The researchers, Khan and his group in 2018 [6] have cited in their study on Empirical Analysis of the Commercial VPN Ecosystem that some of the countries allow only the government-approved VPN providers, while some countries allow the VPN use only to certain institutions such as banks. The VPN services are also

used to get access to the geo-filtered content and download the copyrighted materials. The users deploy VPN services to shield their IP address when using peer-to-peer systems.

The critical resources of the phones are protected by using the permission security model in the android phones, in which the application prompts for permission to access the critical resources during the installation process. It is presumed that the user knows the risks involved in granting these permissions to the applications. However, in contrast, the lack of knowledge or awareness of the user, the malware becomes successful in gaining access to the phone's resources and performs malicious activities such as stealing the personal data thereby affecting the users even financially[7]. An online survey conducted by Clement [8] among internet users worldwide in the first quarter of 2018, found out that 26% of the respondents used VPNs and proxy servers to access the internet. 30% of the users were in the Asia Pacific region, which was ranked the highest among the regions.

As stated by [9], Google introduced native platform support for VPN clients through the VPN Service base class and its associated BIND_VPN_SERVICE permission in Android version 4.0. It was also emphasized that permission is a powerful Android feature that could be abused by the developers to allow the requesting app to intercept, manipulate and forward the users' traffic to a remote VPN or proxy server of their choice.

As Android smartphones with the VPN apps installed are being used for browsing, accessing online banking services, storing personal data, and so on, the VPN apps can also exfiltrate confidential user data. On the other hand, as VPN apps are being used for providing anonymity while being online, users with a criminal mind can misuse the app to perform illegal activities and are expected to be shielded from the investigators.

This paper analyzes the permissions and the malware content of 229 android VPN apps, and it also tries to study the possibility of finding the forensic artifacts which could be left by the VPNs on the devices. Further, as a part of a privacy study, the DNS leak tests and traffic encryptions are also performed on the selected VPN apps.

1.1 Motivation and Problem Statement

The Google Play Store is hosting a huge list of free applications for android phones to be downloaded by the users and installed readily. In which the VPNs are also included as free and commercial based android apps in the Play Store. The so-called free android VPNs available on the Google Play Store are questionable from the security and privacy perspective.

According to the study conducted by [9], it was found that the users of the VPNs whether free or commercial ones are not aware of the security and privacy implications of the use of such free VPNs readily available on the Google Play Store.

The users of the VPNs are seeking censorship circumvention, online anonymity, and the kind of protection from monitoring and tracking. On the other hand, the VPN providers are making bold claims regarding their ability to fulfill the needs of the users such as censorship circumvention, anonymity, and protection from monitoring and tracking, which the users easily believe to be true.

There are many works carried out on android app forensics but specifically, there is no study done on the possibility of android VPN forensics and also the study of the behavior of the Free android-based VPNs concerning the handling of the user data. The Free VPNs are also alleged to be embedded with malware which could compromise the security and privacy of the VPN users as well as the user data. So, there is also a need to study the possibility of the malware presence on the Free VPN apps.

1.2 Objectives

The main objective of the study was to carry out the forensic and behavioral analysis of the free Android VPN apps guided by the following objectives:

- Find out the VPNs which are using the dangerous level permissions.
- Find out the possible malware content.
- Study the usability of free android VPNs in terms of providing security and privacy.
- Find out if any forensic evidence can be left on the phone by Free Android VPNs.
- Enable the general users to have a pre-informed decision on using the VPNs available from the Play Store.

II. BACKGROUND AND LITERATURE

According to [7], there are four levels of android permissions; normal, dangerous, signature, and signature/system. The android permissions of the category dangerous are high-risk permissions and these permissions can allow access to harmful API calls such as sending SMS, access user's private data and take control of the device, etc. Although the alerts are displayed to the users in the form of system dialogs and notifications regarding the risks of the VPN permission, it is noted that the majority of the users haven't understood the technical reasons behind such notifications.

As stated by [9], Google introduced native platform support for VPN clients through the VPN Service base class and its associated BIND_VPN_SERVICE permission in Android version 4.0. It was also emphasized that permission is a powerful Android feature that could be abused by the developers to allow the requesting app to intercept, manipulate and forward the users' traffic to a remote VPN or proxy server of their choice. Although the legitimate android apps would be using the permission for VPN to introduce anonymity for the user while they are online or to access the restricted content, it is seen by the malicious app developers as an opportunity to harvest the users' personal information by abusing the VPN permission.

In an attempt to answer the question "Can VPN be used abusively for illegal activities?", the CyberGhost VPN's support page maintains that it is the person that commits the crime, not the instrument. Further, it questions "Can we commit crimes with a knife?", which of course we can, and just because the knife can be used as the tool to commit the crime, we should not give up using it [10]. Such is the situation when it comes to the usage of VPNs to commit crimes by the users and we can't afford to stop using the handy tools.

Whenever the crimes are suspected to be committed, the VPN logs are requested by the authorities if it is maintained by the provider for the investigation. However, some jurisdictions which have strong privacy legislation impose no data retention requirements. Concerning the assassination case of Ambassador Andrey Karlov, ExpressVPN stated to Turkish authorities in January 2017, that their VPN does not maintain the connection logs of any customer which would enable us to know the specific IP addresses used by the customers. VPNs are first and foremost security tools that help to protect users from being hacked, tracked, monitored, or otherwise compromised. It is stated that they ensure their servers do not contain personal data about anyone's online activity [11].

To test whether the VPN is protecting the user's privacy and security or not, we have to perform the DNS leak test, IP address leak test, and webRTC leak test [12]. In a study carried out by [13] on the selected 14 popular VPN services, it was found that developer-induced bugs and misconfigurations led to IPv6 and DNS leaks. The work of [9] which studied 200 Android VPNs found the presence of malware, traffic leakage and manipulation, and interception of TLS communication. Further, it identified that the Hotspot Shield VPN injected JavaScript codes to redirect the users to the partner companies. Their study found that 75% of the Free VPNs use third-party tracking libraries and 82% request permissions to access sensitive resources including user accounts and text messages.

Most free apps leverage third-party in-app advertising for monetization. To achieve this, app developers need to connect their apps to an ad network, an intermediate platform used for ad delivery [14]. The free VPNs are not free, we pay with our sensitive information, so don't trust for 100% security and privacy [15].
This study focused on the android VPN permissions, malware presence, DNS leaks, and traffic encryption of the selected android based free VPNs.

III. METHODOLOGY

For this research, the study focused on permission analysis, malware presence, DNS Leak Tests, Encryption, Forensic Artefacts, and network behavior analysis; and the following were considered.

3.1 Sample Selection and Download

To get the list of Free VPNs from Google Play, the search feature was used with the keyword "Free VPN" which listed 250 VPNs. The details of the 250 listed apps such as display name of the VPN in the Play store, ratings offered by the users (out of 5), reviews written by the users, VPN app download size (in Megabytes), number of installations, android versions supported, provider of VPN (Developer), official websites associated, email for support (developer or company), address of the developer, URL for app download and the permissions were collected using the Octoparse 7.2.6 (free) and the Web scrapper (browser extension). Since the android apps are not directly downloadable, the online downloader website for APK downloader link https://apps.evozi.com/apk-downloader was used, which generates the downloadable link for the android app. However, due to some unknown reasons, some of the VPN apps were not available for download. From the 250 VPNs listed, only 232 VPNs were downloaded successfully.

3.2 Android Permission Extraction

After downloading the apps were completed, and to read the Androidmanifest.xml file to extract the permissions, the online parsers and manual permission extraction methods were used by decompiling the app with ApkTool. According to [9], the list of permissions of the apps shown in Google Play's profile doesn't necessarily indicate the use of the VPN permission. For this reason, the VPN's permission which was scrapped from Google Play was not taken into consideration for the permission analysis. To extract the permission from the AndroidManifest.xml file of the android VPNs, the online APK Analyzer was used to speed up the process of permission extraction. Besides, the manual process of the permission extraction was also used whenever the online APK Analyzer failed to parse the AndroidManifest.xml file. Out of 232 downloaded VPNs, the AndroidManifest.xml parsing was successful for only 227 VPN apps.

3.3 Malware Presence

To study the presence of malware in the Android VPN apps, VirusTotal's public API was used to automate malware detection. VirusTotal provides more than a hundred antivirus tools, scanning engines, and datasets, which are commonly used to detect malicious apps, executables, and domains [9]. All the downloaded VPN apps (229) were scanned using VirusTotal's online scanning feature.

3.4 Forensic and Network Behaviour Analysis

For forensic artifacts and network behavior analysis, 31 VPNs were selected based on the presence of dangerous permissions and the number of malware presence being detected during the scanning process. After the analysis of the VPN permissions, 20 VPNs had five or more counts of dangerous level permissions, and 11 VPNs that had been detected by 5 or more antivirus engines of the VirusTotal as malicious were selected for the forensic and network behavior analysis.

3.5 DNS Leak Test

Usually, the translation of the domain names to the IP address is carried out by the Internet Service Provider (ISP) but if the VPN is used, the actual IP address of the client is masked to prevent tracking the location. However, translation leaks out of the VPN tunnel exposing the actual IP address and the location of the ISP to the external world which can, in turn, track the client's IP address. To test the DNS leak, after enabling the VPN and connecting to the VPN server which is located outside the country, the dnsleaktest.com was used to perform the standard and the extended tests. The DNS is said to be leaking if the IP address, location, and rest

of the details such as ISP are being matched. To prevent DNS Leaks, use a VPN that has its encrypted DNS system [12]. According to [16], the creator of the DNS leak test, during the DNS leak test, it sends a series of domain names to be resolved within a specific test domain from the client to the configured DNS server. The Standard test performs a round of six queries, while the Extended test performs six rounds of six queries each. The standard test is said to be more than sufficient to detect the DNS leaks if any.

3.6 Network Traffic Capture

To conduct the network behavior analysis, a rooted phone with Android 5.1.1 was used. The android phone was connected to the laptop's hotspot and from the laptop, the network packets were captured using the Wireshark. The capture filter was used to capture only the packets originating from the android phone and destined to the android phone for 15 minutes. The IP addresses assigned to the phone by the hotspot were within the range of 192.168.137.0/24.

3.7 Forensic Analysis

To be able to conduct the forensic artifact analysis on the possible artifacts left by the VPNs on the device after the VPN was installed, enabled, and used, as a part of the test, the website www.gfsu.edu.in was visited and a file GFSU_Presentation.pdf was accessed, and also a simple webpage was accessed to test the encryption.

IV. ANALYSIS AND RESULTS

This section of the paper presents the analysis of the VPN app permissions, malware presence, DNS leak tests, network behavior, and the forensic analysis of the artifacts left by the VPNs on the device.

4.1 Permission Analysis

In total, the permissions of 227 android VPNs were extracted both by using the tools and the manual methods.

- 54.19% of the VPNs had one or more permissions categorized as dangerous in the official Android developer's documentation (123 VPNs).
- A total of 83 VPNs which comprise 36.56% had WRITE_EXTERNAL_STORAGE permission followed by READ_EXTERNAL_STORAGE with 82 (36.12%).
- The location tracking permissions asked by the android such as ACCESS_FINE_LOCATION and ACCESS_COARSE_LOCATION were asked by 14.09% (32 apps) and 16.29% (37 apps) of the total VPNs respectively.
- The highest number of permissions asked in a VPN app was 36 and there were also VPN apps that had as low as 2 permissions being used. The VPN.lat had used 36 permissions while Ultrasurf had 2 permissions.

The other dangerous level permissions asked by the VPN apps included the use of the camera, audio recording, accessing contacts, and getting accounts.

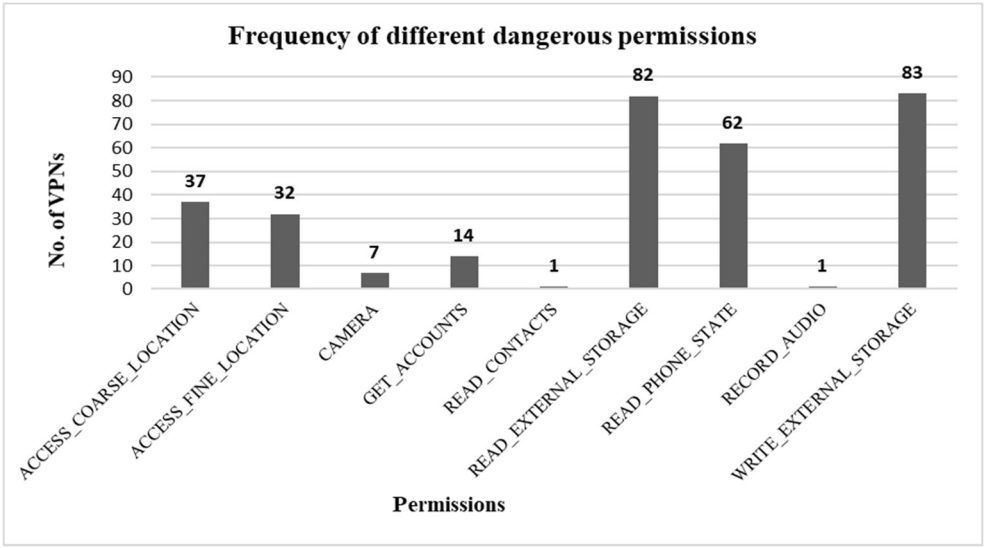

Fig. 1. The number of VPNs using a particular dangerous permission

4.2 Malware Presence

All the downloaded VPN apps (229) binaries were uploaded to VirusTotal's online scanning platform which performs scans using over 60 utilities. After completing the scanning process for a given app, VirusTotal generates a report that indicates which of the participating AV scanning tools detected any malware activity in the app and the corresponding malware signature (if any). The 14.41% (33 out of 229 VPN apps) of the apps were flagged or detected as potential viruses or malware by one or more participating Antivirus scanning tools. The Xiaoming VPN was flagged as malicious the highest (by 8 AV scanners) followed by Unlimited VPN (by 7 AV scanners).

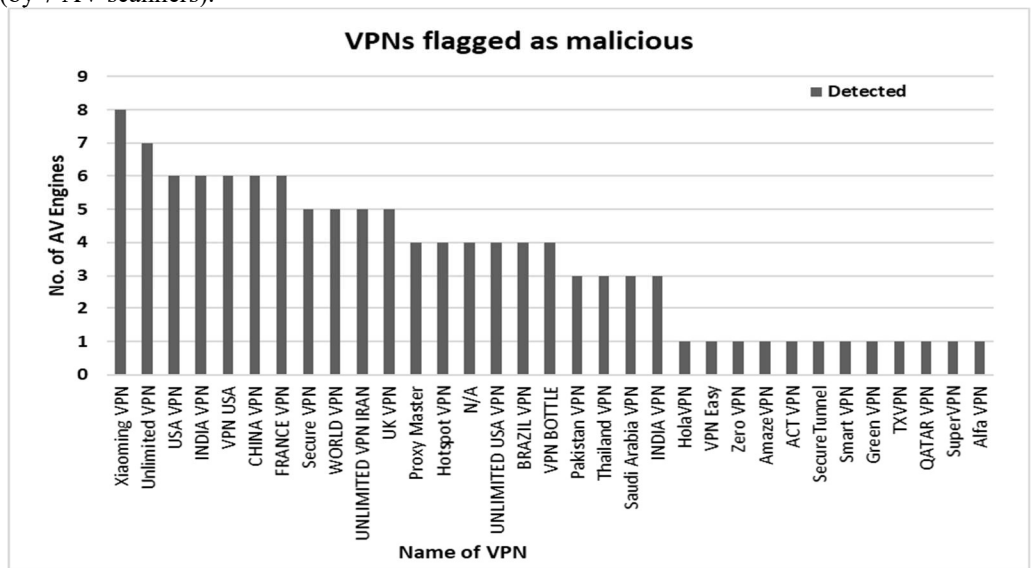

Fig. 2. Number of participating AntiVirus Scanners detecting VPN as malicious

4.3 Forensic and Network Behaviour Analysis

For forensic artifacts and network behavior analysis, 31 VPNs were selected based on the presence of dangerous permissions and the number of malware presence being detected during the scanning process. After the analysis of the VPN permissions, 20 VPNs that had five or more counts of dangerous level permissions and 11 VPNs that had been detected by 5 or more antivirus engines of the VirusTotal as malicious were selected for the forensic and network behavior analysis. Some VPNs which required the payment to be made were excluded while some VPNs which allowed it to be used as a trial for a limited time were included.

From the list of 31 VPNs which were chosen to be used for the forensic and behavior analysis, 21 failed to work in the study environment setup due to a couple of reasons such as not being able to install on the testing device (Sony Xperia, Android Version 5.1.1) used for the study, failed to launch after the installation, not able to connect to the servers, some stopped running when launched and some failed for unknown reasons. In the following Table I and II, the VPNs which could not be tested for the study due to the above-cited reasons are indicated as *"Failed"* against their names. So, out of the 31 listed VPNs, only 10 were able to be successfully used for the DNS Leak Test, encryption, and forensic analysis.

TABLE 1. List of VPNs Flagged as Malicious by 5 or More Antivirus Scanners

SL. No.	VPN Name	Detected by AVs (Nos.)
1	Xiaoming VPN	8
2	Unlimited VPN *(Failed)*	7
3	USA VPN *(Failed)*	6
4	INDIA VPN *(Failed)*	6
5	VPN USA	6
6	CHINA VPN	6
7	FRANCE VPN	6
8	Secure VPN (Premium with trial)	5
9	WORLD VPN	5
10	UNLIMITED VPN IRAN	5
11	UK VPN	5

TABLE 2. List of VPNs with 5 or more dangerous permissions being used

SL. No.	VPN Name	No. of Dangerous Permissions
1	Hi VPN *(Failed)*	6
2	Green VPN *(Failed)*	6
3	TXVPN *(Failed)*	6
4	Opera *(Failed)*	5
5	HolaVPN *(Failed)*	5
6	SuperVPN *(Failed)*	5
7	SpeedVPN *(Failed)*	5
8	Yoga VPN *(Failed)*	5
9	Melon VPN *(Failed)*	5
10	FlashVPN *(Failed)*	5
11	VPN Master *(Failed)*	5
12	GeckoVPN *(Failed)*	5
13	VPN Master (30 minutes time limit)	5
14	LinkVPN *(Failed)*	5
15	MoonVPN *(Failed)*	5
16	Seed4.Me VPN *(Failed)*	5
17	VPN Express *(Failed)*	5
18	VPN EARTH *(Failed)*	5
19	VPNova	5
20	VPN BOTTLE *(Failed)*	5

4.4 DNS Leak Test

From the 10 VPNs used for the test, 2 VPNs were supposed to be the premium but allowed users for a certain period as the trial had DNS leaks. This security flaw occurs when the VPN fails to send the DNS requests via its encrypted tunnel to its DNS servers and permits the DNS requests to be made to the ISP's DNS servers. Even if the users' traffic is concealed, the DNS leaks would expose the browsing history of the users to their ISP which defeats the essence of using the VPN itself.

TABLE 3. List of VPNs Showing the DNS Leak Test Result

SL. No.	VPN Name	DNS Leak Test
1	Xiaoming VPN	No DNS Leak
2	VPN USA	No DNS Leak
3	CHINA VPN	No DNS Leak
4	FRANCE VPN	No DNS Leak
5	Secure VPN (Premium with trial)	DNS Leak
6	WORLD VPN	No DNS Leak
7	UNLIMITED VPN IRAN	No DNS Leak
8	UK VPN	No DNS Leak
9	VPN Master (30 minutes time limit)	DNS Leak
10	VPNova	No DNS Leak

4.5 Traffic Encryption

The VPN is supposed to create an encrypted VPN connection successfully between the device and the server; it was found that only 9 VPNs out of 10 created encrypted connections; 1 VPN app was sending the traffic without any encryption. The encryption of each of the VPN app was tested by creating a VPN connection on an isolated network and using Wireshark to capture the traffic while accessing the web page. We then analyzed the data we had captured for any unencrypted content from that page.

TABLE 4. List of VPNs Showing the Encryption Results

SL. No.	VPN Name	Encryption
1	Xiaoming VPN	Encrypted
2	VPN USA	Encrypted
3	CHINA VPN	Encrypted
4	FRANCE VPN	Encrypted
5	Secure VPN (Premium with trial)	Encrypted
6	WORLD VPN	Encrypted
7	UNLIMITED VPN IRAN	Encrypted
8	UK VPN	Encrypted
9	VPN Master (30 minutes time limit)	Unencrypted
10	VPNova	Encrypted

4.6 Forensic Analysis

Due to the misconfigurations and underlying flaws, the VPNs can leave artifacts that could be used to confirm or corroborate the evidence. When the possible artifacts were looked for, 7 VPNs out of 10 had an android.conf file stored in the cache directory. The android.conf file had details such as Private Key, Public Key, Certificates, Digital Signature, etc besides other information that may be useful for investigative tasks.

TABLE 5. Details of VPNs That Had an android.conf File in Cache

SL. No.	VPN Name	Forensic Artifacts
1	Xiaoming VPN	No
2	VPN USA	android.conf file
3	CHINA VPN	android.conf file
4	FRANCE VPN	android.conf file
5	Secure VPN (Premium with trial)	android.conf file
6	WORLD VPN	android.conf file
7	UNLIMITED VPN IRAN	android.conf file
8	UK VPN	android.conf file
9	VPN Master (30 minutes time limit)	No
10	VPNova	No

V. DISCUSSION

The dangerous category of android permissions can be used both by benign and malicious android applications. From the total of 227 VPNs used for the permission analysis, it was found out that 54.19% of the VPNs had one or more permissions categorized as dangerous as per the official Android developer's documentation. The permissions included accessing the coarse location, accessing the fine location, using the camera, reading contacts, reading external storage, writing to external storage, recording audio, and getting accounts.

The WRITE_EXTERNAL_STORAGE permission was used by 83 VPNs followed by the android permission READ_EXTERNAL_STORAGE (82 VPNs). It was not evident whether these permissions are misused or not but because the majority of the VPN apps are made free for the users, a large number of users are attracted and it is important that the user cast some doubts.

The highest number of permissions asked in a VPN app was 36 and there were also VPN apps that had as low as 2 permissions being used. The VPN.lat had used 36 permissions while Ultrasurf had 2 permissions. However, it is important to note that the number of permissions asked or used in a VPN app would correspond with the features and functions provided by the app. The 14.41% (33 out of 229 VPN apps) of the apps were flagged as potential viruses or malware by one or more participating Antivirus scanning tools but the false positives could not be ascertained. The Xiaoming VPN was flagged as malicious the highest (by 8 AV scanners) followed by Unlimited VPN (by 7 AV scanners). The VPNs which were flagged by more antivirus scanners should be used with restraint. By using the permissions which are not required for the app and by embedding the malicious codes, the users' data and information can be misused or put at risk.

Although the DNS leaks and failed encryption can't be intentional, out of 10 VPNs tested, two had DNS leaks and on the other hand, one failed to tunnel and encrypt the traffic sent to and from the device. Such failures would put the users on the disadvantage side and the essence of using a VPN for security and privacy would be defeated.

It is not only the developers who can misuse the VPN but also the users with criminal intent can use the VPN for carrying out the malicious tasks and expect to be shielded from the investigations. In an attempt to find out if any artifacts of forensic value could be left by the chosen VPNs, the android.conf file was found stored in the cache directory of the 7 VPNs which may be useful in investigations. The android.conf file containing information such as Private Key, Public Key, Certificates, Digital Signature, etc. but the forensic and investigative value of the file could not be determined.

It was not ascertained how the android.conf file can be used by the investigators in case if the crime is committed using the free Android VPNs, and how valuable the android.conf file can be. However, detailed

work has to be carried out to find out whether or not the file is valuable from the forensic and investigative perspective.

5.1 Limitations and Future Work

The free Android VPN forensic and behavioral analysis study was carried out with several limitations. The first limitation was the coverage of the free android VPNs; the attempt to get all the free Android VPNs listed from the Google Play store was made with the keyword "Free VPN" and only the apps which got listed were considered for the study. The keyword "Free VPN" could have missed apps. From the listed VPN apps, some VPNs could not be downloaded which led to the reduction in the number of VPNs chosen for the study. When it comes to testing the DNS leaks, encryption, and forensic artifacts, all the VPNs could not be studied due to the large amount of time required to be spent on each chosen VPN.

For this study, the device used for testing the VPNs was a rooted Sony Xperia device with android version 5.1.1, which failed to support some VPN app installation. The devices chosen for the study could have been more in numbers to be more resilient.

While capturing the traffic to and from the device, the time limit was set to just 15 minutes which could have been longer to enable the study of behavior, and the sample size for the DNS leak test and the VPN traffic encryption was very small; the tests could have been conducted for all the VPN apps.

The presence of android.conf file found in the cache directory of 7 Free VPNs was captivating because it had information such as the private key, public key, digital signature, etc. In the future, as a part of forensic analysis, the android.conf file contents could be studied to determine whether or not the file possesses forensic and investigative value.

VI. CONCLUSION

The study revealed that the majority of the Android-based VPNs have intrusive permission which can be dangerous for the users and at the same time some of the VPNs were flagged for the presence of possible malware content; besides, some of the Free VPNs even failed the DNS leak tests and traffic encryption checks. While some of the Free VPNs seemed to have no issues with the current set of checks performed, it is hard to endorse that such VPNs are not malicious. Given the availability of Free VPNs which can be readily downloaded from the Google Play store, the users must be aware of the inherent risks; not all the VPNs which help circumvent censorship or to access geo-blocked content provide security and privacy.

REFERENCES

[1] S. Bommisetty, R. Tamma, and H. Mahalik, *Practical Mobile Forensics*. Birmingham B3 2PB, UK: Packt Publishing Ltd., 2014.

[2] R. Brandom, "There are now 2 . 5 billion active Android devices," 2019.

[3] G. Dautovic, "Android Market Share : The Fight for Mobile Leadership Top Android Companies by Market Share," 2019. [Online]. Available: https://fortunly.com/blog/android-market-share/.

[4] Ivar, "Why you shouldn't trust all VPNs on Google Play Store," 2019. [Online]. Available: https://hackernoon.com/why-you-shouldnt-trust-all-vpns-on-google-play-store-w623i3286. [Accessed: 20-Nov-2019].

[5] J. Roach, "The Worst Free VPN Providers of 2019: Keep Away From These Services," 2019. [Online]. Available: https://www.cloudwards.net/worst-free-vpn/.

[6] M. T. Khan, A. C. Snoeren, J. DeBlasio, C. Kanich, G. M. Voelker, and N. Vallina-Rodriguez, "An empirical analysis of the commercial VPN ecosystem," *Proc. ACM SIGCOMM Internet Meas. Conf. IMC*, pp. 443–456, 2018.

[7] S. Malik and K. Khatter, "Behaviour analysis of android application," *Int. J. Control Theory Appl.*, vol. 9, no. Specialissue11, pp. 5307–5322, 2016.

[8] J. Clement, "Global VPN usage reach 2018, by region," 2019. [Online]. Available:

https://www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/. [Accessed: 21-Nov-2019].

[9] M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An analysis of the privacy and security risks of android VPN permission-enabled apps," *Proc. ACM SIGCOMM Internet Meas. Conf. IMC*, vol. 14-16-Nove, pp. 349–364, 2016.

[10] CyberGhost VPN, "Can CyberGhost VPN be used abusively for illegal activities?," 2019. [Online]. Available: https://support.cyberghostvpn.com/hc/en-us/articles/214013865-Can-CyberGhost-VPN-be-used-abusively-for-illegal-activities. [Accessed: 21-Nov-2019].

[11] ExpressVPN, "ExpressVPN statement on Andrey Karlov investigation," 2019. [Online]. Available: https://www.expressvpn.com/blog/expressvpn-statement-andrey-karlov-investigation/. [Accessed: 22-Nov-2019].

[12] vpnMentor, "How to Test Your VPN ' s Security (Updated 2019)," 2019. [Online]. Available: https://www.vpnmentor.com/blog/test-vpn-security/. [Accessed: 22-Nov-2019].

[13] V. C. Perta, M. V. Barbera, G. Tyson, H. Haddadi, and A. Mei, "A Glance through the VPN Looking Glass: IPv6 Leakage and DNS Hijacking in Commercial VPN clients," *Proc. Priv. Enhancing Technol.*, vol. 2015, no. 1, pp. 77–91, 2015.

[14] B. He, H. Xu, L. Jin, G. Guo, Y. Chen, and G. Weng, "An Investigation into Android In-App Ad Practice: Implications for App Developers," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, 2018, vol. 2018-April, pp. 2465–2473.

[15] Tenta, "The Dangers Of Free VPNs - What You Need To Know," 2018. [Online]. Available: https://tenta.com/blog/post/2018/02/the-dangers-of-free-vpn. [Accessed: 08-Apr-2019].

[16] J. Campbell, "Standard vs Extended test," 2019. [Online]. Available: https://www.dnsleaktest.com/what-is-the-difference.html. [Accessed: 22-Nov-2019].