Analysis of VirusTotal Android Application

Varun Patil
(vcpatil)

15th December 2014.

Abstract:

VirusTotal is a subsidiary of Google. It is an online tool that allows the user to scan its files and URLs. VirusTotal will analyze these URLs to identify virus, worms, Trojans and other kind of malicious concerns.

VirusTotal uses a combination of anti-virus products for the analysis of these files. Hence, with the help of VirusTotal it can be possible to check for false positives. False positives occur when some of the applications raise a red flag over an otherwise innocuous application. There is a higher possibility of there being a false positive during analysis of VirusTotal due to vast variety of anti-virus products it uses to obtain the results.

Therefore the plan in this research is to search for some of the most popular application which one can assume are safe and test them using VirusTotal Android Application. During, this process we can identify whether a particular application is malicious or false positive based on the number of anti-virus vendors that report it as malicious.

Based on this research we can identify the credibility of VirusTotal. Also, by the end of the research we will be having the numbers to support the claim.

1. Introduction:

VirusTotal is a non-commercial website which is the subsidiary of Google. It enables a user to check for viruses, worms, Trojans and other malicious content within a particular file or an URL [1].

VirusTotal has a web application as well as an android application. The web application has an interface where the user can provide the URL of a website that he wants to scan for threats. The website will be scanned by VirusTotal using the collection of anti-virus products that it has at its disposal. The scan reports will be generated within seconds. Also, when the user enters the link of the website to be scanned, he will be notified about the last time a scan was carried out on the same website using VirusTotal. Hence in cases where the last scan was carried only moments ago, the user will be saved of the effort to carry out the tests again.

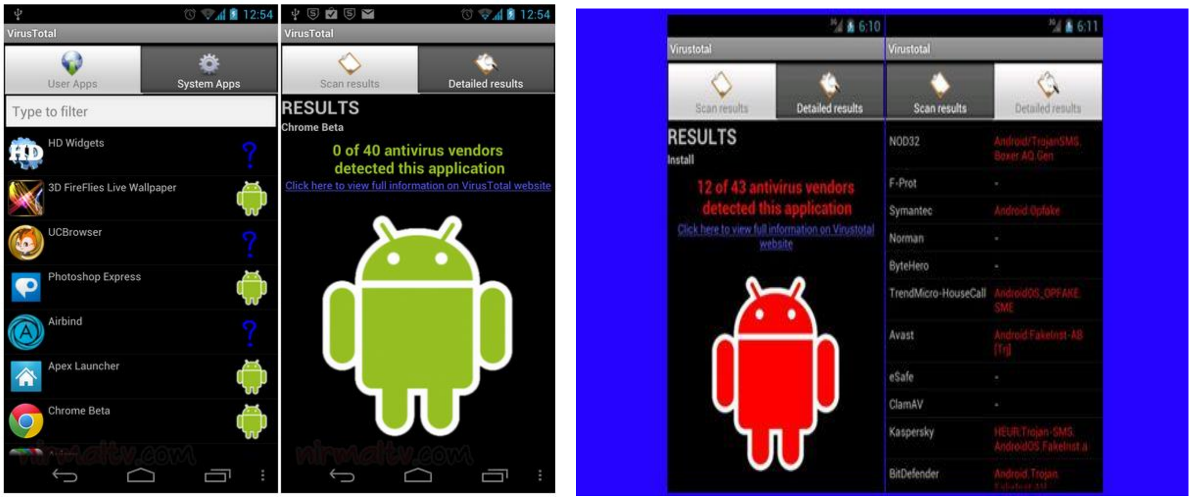
If the user wants to scan a particular file on his system then he can upload on the VirusTotal website, and the results of the scan will be displayed on the website within seconds. Another option offered to the user is of using the e-mail service. The user can e-mail the file he wants to scan. The results of the scan will be conveyed to the user via responding e-mail.

The android application for VirusTotal is available on the Play Store. The application has already had more than six thousand downloads [2]. The application mainly feature two main pages. The first page is the home page where the list of the application is maintained. The applications that are yet to be tested have a question mark besides it as shown in the Figure 1(a). The application which are tested and were not detected malicious by any of the 64 anti-virus vendors have a green android icon besides them as depicted in Figure 1(b). The application that have been detected as malicious will have a red icon accompanying it as shown in the Figure 1(c).

The second page carries the result of the tests. This page has two tabs, one of them is the scan results tab which shows how many of the anti-virus vendors detected the application as malicious out of the total number of anti-virus vendors that scanned the application. This page also provides the link to view the detailed results of the scan on the VirusTotal Website. The other tab is named the detailed results which carries the list of the vendors that were involved in the scanning process. If an anti-virus product detects the application as malicious, the detailed results tab will contain the name of the Trojan, worm or virus which caused the anti-virus vendor to raise the flag.

It has been reported by one of the security vendors that number of mobile application which are inflicted by malware or are conduits of spyware has nearly quadrupled from the year 2011 to 2013 [3]. The most surprising part is that most of the applications were still available on the Google's Play store at the time of reporting. In another article it was published there are 1730 Android applications that are still at large in the market [4].Almost 500 of these applications are still on the Google Play Store. Also, it has been largely observed that the Google Play Store is not as carefully regulated as the Apple App Store. Thus, raising the question of the security procedure undertaken by Google before the application is released on the Play Store. VirusTotal uses the combination of more than 56 anti-virus product.

In this paper, the design and implementation, evaluation, related work and the future scope of the research is represented in the successive sessions.



0 of 40 antivirus vendors detected this application

12 of 43 antivirus vendors detected this application

NOD32	Android/TrojanSMS.Boxer.AQ.Gen
F-Prot	-
Symantec	Android.Opfake
Norman	-
ByteHero	-
TrendMicro-HouseCall	AndroidOS_OPFAKE.SME
Avast	Android:FakeInst-AB [Trj]
eSafe	-
ClamAV	-
Kaspersky	HEUR:Trojan-SMS.AndroidOS.FakeInst.a
BitDefender	Android.Trojan.

(a) (b) (c) (d)

Figure 1

2. Design and Implementation

In my efforts, to scan the effectivity of VirusTotal android application, the application were downloaded from the Google Play Store and scanned on an Android device. The device used in this case was HTC Explorer. The device uses Android OS, v2.3 (Gingerbread).

There were a lot of limitations that were caused by using this model of android phone. Since the phone only has 90 Mb of internal memory [5], the test could be carried out for only one application at any time. This made the process of testing very slow. Also, since this phone belongs to the previous generation of Android Phones, there were compatibility issues with the Google Play store forcing me to engage in the updating of the Google Market and the concerned applications. With the availability of only 512 MB RAM, the computation power was also significantly reduced.

In order to make the research pertinent to the current situation, it was mandatory to collect a reasonable dataset of applications. For this purpose the list of the most downloaded applications [6] was obtained from the sources. Additionally we also the most recommended applications of the year 2013 and 2014 to our dataset. Apart from this there was a necessity to test the applications that have been publicized as having malicious properties to this dataset. In case of absence of such applications, the tests were performed on the namesakes of this application in order to confirm that there is no existence of any such applications on the Play Store. It can be noted that all the application used to carry out the experiments were downloaded from the Google Play Store as the applications from the third party stores could not be trusted. As per the selection criteria, 227 application from the Google Play Store were selected for the tests.

Once the applications are downloaded on to the android phone, we open the VirusTotal android application. The recently downloaded applications occur in a list with a question mark at the end of that row signifying that the application is yet to be tested.

3. Evaluation:

Once we click on the icon of the application to get it tested, the results of the test are usually generated within a couple of seconds. The following bar-chart summarizes the results observed during the tests.

From the statistics mentioned in the figure2, it can be safely assumed that the VirusTotal android application is successful in detecting the malicious content as the dataset mainly comprised of some of the most downloaded application which are developed by some of the top developers on Play Store. However, further analysis into the applications, reported as malicious, provides us with some startling observations.

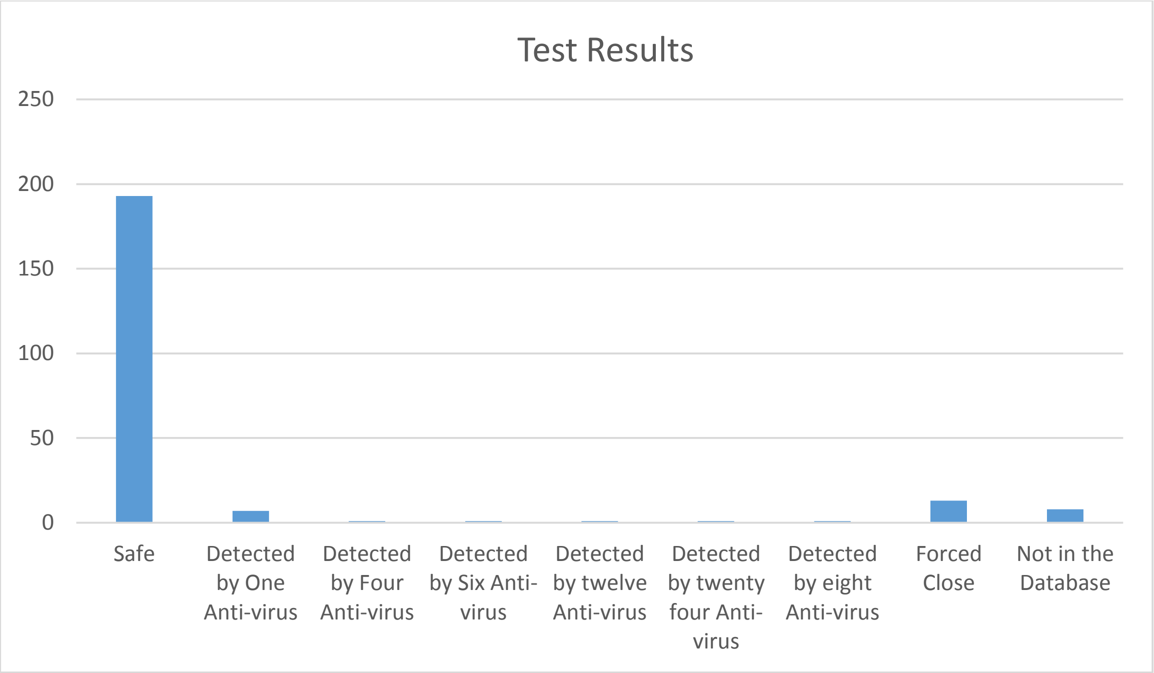


Figure2

It is worth noting that the application Yelp, which is developed by Yelp Inc. [11] and is one of the most downloaded application on the Google Play store was reported that by VirusTotal. NANO-Antivirus was the only one antivirus vendor out of the fifty four vendors that were included in the test that detected this application as malicious. The threat reported was Trojan.Android.Uten.dhstuc. It is worth noting that this application has been wrongly reported by VirusTotal and is a false positive. The table below presents a list of applications that were reported by VirusTotal.

Name of the Application	Number of Vendors in the test	Number of Vendors who reported maliciousness	Names of the vendors	Detection
Yelp	54	1	NANO-Antivirus	Trojan.Android.Uten.dhstuc
My Talking Tom	55	1	Aegis Lab	suspicious
Talking Tom Cat 2 Free	54	6	Aegis Lab , TrendMicroHousecall, Sophos, Avira, ESETNOD32,Fortinet-	Suspicious, Suspicous_GEN.F47V0908, Android MultiAds, Adware/ANDR.Domob.H. Gen, a variant of Android/Domob.G, Adware/Domob!android
TV90Ultimate	1	55	NANO-Antivirus	Trojan.Android.Fatakr.dapbon
Pool Billiards Pro	1	56	Kingsoft	Android.Troj.luomao.cr.(kcloud)
Angry Birds Go!	1	53	AegisLab	admob_1

Subway Surfers Free tips	8	54	McAfee, NANO, Antivirus, Comodo, Sphos, VPIRE, Avware, ESET-Nod32, Ikarus	Artemis!5f2DE15C0653, Riskware.Android.Airpush.ddwkzc, ApplicUnwnt, Android Multi Ads, Adware.AndroidOS.Youmi.Startapp (v), Adware.AndroidOS.Youmi. Startapp (v), a variant of Android/AdDisplay.Startapp.B, Adware.AndroidOs.Startapp
Wallpapers QHD	4	54	AegisLab, Aegis Lab , TrendMicroHousecall, Sophos	admob_1, Suspicious, Suspicous_GEN.F47V0908, Android MultiAds, Adware/ANDR.Domob.H.
NBA Squadre Puzzle Game	1	55	Nano Antivirus	Trojan.Android.Dowgin.dfewcg
Everywhere for tinder	1	53	AegisLab=	admob_1
liveLocker	24	54	https://www.virustotal.com/en/file/4d2f02ebda35e280e65362ade160d34d84ef421c/analysis/	https://www.virustotal.com/en/file/4d2f02ebda35e280e65362ade160d34d84ef421c/analysis/
Any Video Converter	1	54	McAfee, NANO-Antivirus, TrendMicro-HouseCall, Comodo, VIPRE, ESET-NOD32 , AVware, Avira, Sophos, AVG, Fortinet	Artemis!1E991AF26200, Trojan. Android.Leadbolt.dgrynq, Suspiciou_GEN.F47V1104, ApplicUnwnt, DrWeb-Adware.Leadbolt.9.origin, Adware.AndroidOS.LeadBolt.a (v), Android LeadBolt, Avira-Adware/ANDR.Leadbolt.B.Gen, AVware Adware.AndroidOS.LeadBolt.a (v), a variant of Android/Leadbolt.E, Adware/LeadBolt!Android, Android/Deng.BOD

Table 2

In case of the detected vulnerabilities, VirusTotal was successful in detecting the malicious applications like LiveLocker and Subway Surfer Free tips which are widely publicized as malicious [3]. However while Talking Tom Cat Free is publicized to have some safety issues, this application was not found in the database of VirusTotal [12]. On the other hand its other versions like My Talking Tom and Talking Tom Cat 2 Free were identified as malicious.

There have been cases where the application force closes. However, when we reopen the application the android icon accompanying the application, that cause the force closure, is turned either green or red or in some cases it continues to be a question mark suggesting that the application was not found in the database at VirusTotal. However, in such a case even if the application is detected by VirusTotal we do not get the statistics associated with the application making it difficult to classify false positives.

4. Related Work:

Considering the fact that VirusTotal was launched way back in 2004. It is very surprising that there has been no research on this topic. It may seem that the researchers out there don't realize the potential that the statistics on the analysis of the results produced by VirusTotal may have.

There can be another side to this argument. The researchers may have failed to notice that an application such as VirusTotal could be a source of false positives. Consequently, they may be taking the effectiveness of VirusTotal for granted.

5. Conclusion:

The application is successful in correctly identifying some of the malicious applications and rightly reports many of the application as safe. However, there have been cases where the application shows false positives especially in the case of Yelp. Also, the force closing of the application is confusing, how are the scans able to detect an application as malicious if they do not properly show the vendor statistics and the reported detections. Additionally, there is a need for VirusTotal to increase the number of applications in its database as even the widely used application like Talking Tom and BCCI is not in the database at VirusTotal.

Another interesting aspect was the finding that Google has still not removed some of the malicious application like LiveLocker from the Play Store.

6. Future Work:

The project can be tested further by implementing the tests on the newer batch of the application. For this it is mandatory that the new applications be included in the VirusTotal database. Also, there can be a communication link with Google that alerts them about the reported vulnerabilities and enables them to employ some stricter checks on the applications in the Google Play Store. With the increasing number of Android users this step is mandatory to curtail the number of malicious attacks on android applications.

Resources:

[1] https://www.virustotal.com/en/about/

[2] https://play.google.com/store/apps/details?id=com.virustotal&hl=en

[3] http://www.infoworld.com/article/2610099/mobile-security/report--android-malware-and-spyware-apps-spike-in-the-google-play-store.html

[4] http://blog.trendmicro.com/trendlabs-security-intelligence/1730-malicious-apps-still-available-on-popular-android-app-providers/

[5] http://www.gsmarena.com/htc_explorer-4102.php

[6] http://en.wikipedia.org/wiki/List_of_most_downloaded_Android_applications

[7] http://www.techradar.com/us/news/phone-and-communications/mobile-phones/top-210-best-android-apps-2013-693696

[8] http://www.techradar.com/us/news/phone-and-communications/mobile-phones/60-best-free-android-games-2013-687718

[9] http://www.pcmag.com/article2/0,2817,2393097,00.asp

[10] http://www.howtogeek.com/188519/how-to-tell-if-an-android-app-is-potentially-dangerous/

[11] https://play.google.com/store/apps/details?id=com.yelp.android&hl=en

[12] http://www.ijailbreak.com/android/trustgo-halloween-spotlight-infographic/

[13] http://www.androidauthority.com/malware-up-580-percent-126373/