There are big differences in reliability when comparing mobile security vendors.

I am a procurement staffer at an IT company in Silicon Valley. Recently, our company required a new mobile security vendor so I have conducted a comparison of the cybersecurity providers on the market today.

The results are unexpected. Apparently, the most reliable providers are not the most well known, but rather stealth players from Slovakia, Korea, India, and a startup from United States. So please do your research before placing an order, especially when the outcome can affect your promotion.

Now, let me show you which tests we did, and the results we gathered.

We collected most of our testing data from VirusTotal (VT). VT is a website which hosts many antivirus scanners. Users can upload different types of files including exe, dll, pdf, doc, ppt, apk and so on to VT and it will return scan results from all of the hosted vendors. VT was founded in 2004 and then was acquired by Google in 2012. Now, VT hosts 60+ antivirus engines, which scans millions of samples submitted by users daily from all over the world. All of the scan reports are shared with the public VT community. These test results may be verified by querying the testing samples on VT.

To perform the tests, I needed to prepare benign and malicious samples. Our company has some benign APK samples, but no malicious samples. Fortunately, VT provides an API to get a live feed with the latest samples submitted to VT. So we upload our benign APK samples to VT to see if any vendor will misclassify them as malware. From the live feed samples, we also select some malicious APK samples and benign APK samples using a very conservative labeling policy. First we label samples with a high positive rate as malware; a sample gains a positive when an antivirus engine flags it as malware. Next we label a sample as benign if it has a very low positive rate, has been scanned multiple times, and has been in VT for at least a few months. Additionally, we also use an open source tool called AVPASS to obfuscate some of the same malware and re-submit them to VT to see if the antivirus engines can still recognize them.

Using the method above, we can build a testing dataset with minimum false positive and false negative. Each day, we prepare such a dataset to test antivirus vendors' performance. We tested 66 vendors for a period of 14 days: from 11/01 to 11/14. The final results are shown in the following table, and reflect averaged daily results. There are 9 columns in total:

- Vendor: antivirus vendor's name
- Country: antivirus vendor's country
- Total: total number of testing samples
- TN: True Negative, number of negative (benign) samples being correctly predicted as negative
- FN: False Negative, number of positive (malicious) samples being mispredicted as negative
- FP: False Positive, number of negative samples being mispredicted as positive
- TP: True Positive, number of positive samples being correctly predicted as positive
- TPR: True Positive Rate, percentage of positive samples being correctly predicted as positive
- FPR: False Positive Rate, percentage of negative samples being mispredicted as positive.

Consequently, an antivirus engine is considered good only if it has a high TPR (so it can detect more malware) and low FPR (so it has less false alarm).

Averaged Daily Test Results for APK from VirusTotal (11/01/2018-11/14/2018)								
Vendor	**Country**	**Total**	**TN**	**FN**	**FP**	**TP**	**TPR**	**FPR**
ESET-NOD32	Slovakia	21885	17353	63	55	4,414	98.69%	0.38%
Trustlook	United States	21885	17387	66	21	4,411	98.33%	0.12%
AhnLab-V3	Korea	21885	17384	148	24	4,329	96.73%	0.18%
K7GW	India	21885	17307	178	100	4,299	96.09%	0.77%
Ikarus	Austria	21885	17344	223	63	4,254	94.86%	0.47%
Fortinet	United States	21885	17407	274	1	4,203	94.37%	0.00%
ZoneAlarm	United States	21885	17395	299	13	4,178	93.37%	0.07%
Kaspersky	Russia	21885	17396	306	12	4,171	93.23%	0.07%
CAT-QuickHeal	India	21885	17299	755	109	3,722	86.40%	0.84%
Sophos	United Kingdom	21885	17397	712	11	3,765	85.98%	0.09%
MAX	India	21885	17407	935	0	3,542	81.94%	0.00%
BitDefender	Romanian	21885	17406	954	2	3,523	81.60%	0.01%
Emsisoft	New Zealand	21885	17406	953	2	3,524	81.58%	0.01%
GData	Germany	21885	17405	981	2	3,496	80.96%	0.01%
Ad-Aware	Canada	21885	17406	1003	1	3,474	80.33%	0.00%
MicroWorld-eScan	India	21885	17407	1036	1	3,441	79.62%	0.00%
Arcabit	Poland	21885	17406	1101	2	3,376	78.41%	0.01%
F-Secure	Finland	21885	17398	1096	10	3,381	78.17%	0.08%
NANO-Antivirus	Russia	21885	17384	1189	24	3,288	77.40%	0.19%
DrWeb	Russia	21885	17252	1293	156	3,184	76.06%	1.20%
Cyren	Israel	21885	17331	1328	76	3,218	75.47%	0.61%
McAfee	United States	21885	17405	1341	2	3,136	74.49%	0.01%
Avira	Germany	21885	17406	1540	2	2,937	72.01%	0.00%
McAfee-GW-Edition	United States	21885	17406	1568	2	2,909	68.74%	0.00%
SymantecMobileInsight	United States	21885	15821	1880	1587	2,597	62.70%	10.57%
Qihoo-360	China	21885	17292	1975	115	2,502	60.57%	0.68%

AVG	Czech Republic	21885	17402	1992	6	2,485	60.50%	0.04%
Avast	Czech Republic	21885	17402	1993	6	2,484	60.49%	0.03%
Symantec	United States	21885	17402	2100	6	2,377	57.81%	0.04%
Tencent	China	21885	17223	2169	185	2,308	55.69%	1.26%
Baidu	China	21885	17406	2276	1	2,201	53.84%	0.00%
Antiy-AVL	China	21885	17310	2350	98	2,127	51.24%	0.59%
TrendMicro-House Call	Japan	21885	17401	3132	7	1,345	30.86%	0.06%
Microsoft	United States	21885	17406	3484	1	993	24.80%	0.00%
Zillya	Ukraine	21885	17361	3516	47	961	22.57%	0.34%
AegisLab	Taiwan	21885	17157	3537	251	940	21.63%	1.71%
F-Prot	Iceland	21885	17405	3737	2	740	16.61%	0.01%
Zoner	Czech Republic	21885	17406	3774	2	703	16.51%	0.01%
Jiangmin	China	21885	17282	3848	125	629	14.11%	0.87%
ClamAV	United States	21885	17352	4049	56	428	9.81%	0.27%
Kingsoft	China	21885	17398	4106	10	371	8.13%	0.06%
TrendMicro	Japan	21885	17391	4136	16	341	7.64%	0.13%
Rising	China	21885	17397	4178	10	299	6.75%	0.06%
VBA32	Belarus	21885	17403	4314	4	163	3.59%	0.01%
TotalDefense	United States	21885	17408	4385	0	92	2.11%	0.00%
Yandex	Russia	21885	17407	4387	1	90	2.07%	0.00%
Panda	Spain	21885	17407	4402	1	75	1.75%	0.00%
Comodo	United States	21885	17407	4406	1	71	1.61%	0.00%
ViRobot	Korea	21885	17407	4429	1	48	1.05%	0.00%
Alibaba	China	21885	17407	4459	0	18	0.41%	0.00%
AVware	Brazil	21885	17407	4457	1	20	0.41%	0.00%
K7AntiVirus	India	21885	17408	4466	0	11	0.26%	0.00%
ALYac	Korea	21885	17408	4472	0	5	0.10%	0.00%
TheHacker	Bulgaria	21885	17400	4473	8	4	0.10%	0.05%

Invincea	United States	21885	17408	4475	0	2	0.04%	0.00%
Malwarebytes	United States	21885	17408	4475	0	2	0.04%	0.00%
Bkav	Vietnam	21885	17402	4477	5	0	0.00%	0.04%
CMC	Vietnam	21885	17408	4477	0	0	0.00%	0.00%
CrowdStrike	United States	21885	17408	4477	0	0	0.00%	0.00%
Endgame	United States	21885	17408	4477	0	0	0.00%	0.00%
SentinelOne	United States	21885	17407	4477	0	0	0.00%	0.00%
SUPERAntiSpyware	United States	21885	17408	4477	0	0	0.00%	0.00%
VIPRE	United States	21885	17408	4477	0	0	0.00%	0.00%
Webroot	Ireland	21885	17408	4477	0	0	0.00%	0.00%
WhiteArmor	HongKong	21885	17408	4477	0	0	0.00%	0.00%
nProtect	Korea	21885	17408	4477	0	0	0.00%	0.00%

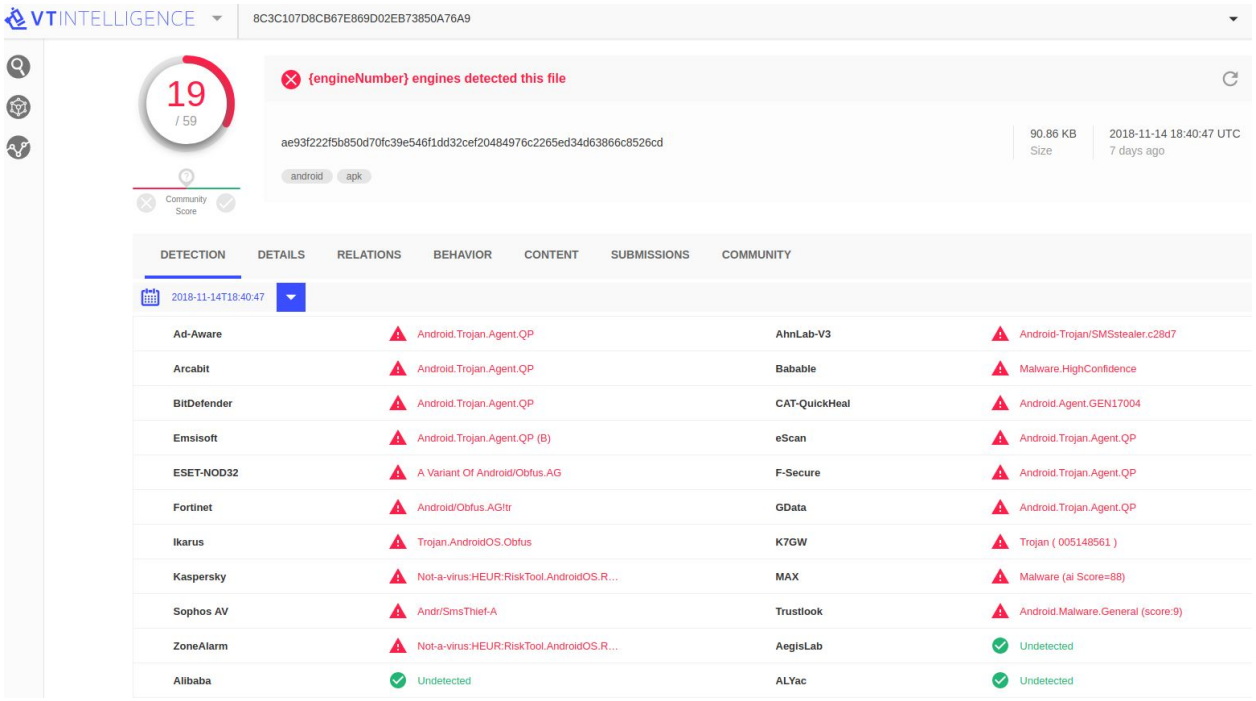
In the table, we sorted the vendors according to their TPR which represents their malware detection capabilities. In total, four vendors have achieved more than 95% detection rate which are ESET-NOD32 from Slovakia, Trustlook from United States, AhnLab-V3 from Korea, and K7GW from India. Among them, Trustlook has the lowest FPR of 0.12%. Among the eight vendors with over 90% TPR, Fortinet has the lowest FPR which is close to 0.

The testing results are a little bit surprising to me. Famous vendors like Avast, BitDefender, McAfee, and Symantec are not even on the Top 20 list in terms of TPR. There are around 20 vendors whose TPR is close to 0, I guess they do not provide APK scanning service. What caught my eye is a startup called Trustlook. I have never heard of this company before, but apparently based on my test, they provide an excellent mobile security service.

I also uploaded an Excel file on github with all my tests results.

https://github.com/alekswicked/VTEngines/blob/master/data/Data_Nov_2018.xlsx

Inside the file, there are 14 worksheets, named after the testing date. In each sheet, the first column is the sample's MD5 hash, the second column is the sample's label, 1 meaning positive (malicious) and 0 meaning negative (benign). The other columns are the vendors' detection results on the samples, 1 means a sample is detected as malware by a vendor. The results can be verified using VT. For example, the first sample on sheet "20181114" with MD5 "8C3C107D8CB67E869D02EB73850A76A9" was detected by Ad-Aware, AhnLab-V3, Arcabit, BitDefender, CAT-QuickHeal, ESET-NOD32, Emsisoft, F-Secure, Fortinet, GData, Ikarus, K7GW, Kaspersky, MAX, MicroWorld-eScan, Sophos, Trustlook, and ZoneAlarm. If you search the sample on VT, you will find something like this:



It shows, the file was scanned on 2018-11-14 18:40:47 UTC and detected by the vendors listed before.

In conclusion, if you need mobile security service, I recommend you to select from ESET-NOD32, Trustlook, AhnLab-V3 and K7GW.