Supplementary Report to the File Detection Test of September 2015

Language: English
September 2015
Last Revision: 12th November 2015

Commissioned by Microsoft

www.av-comparatives.org

Introduction

Microsoft commissioned this supplementary report. This support from Microsoft provided extra funding enabling us to build a new model for scoring vendors using malware prevalence. Microsoft also provided the detailed global threat telemetry required to prevalence-weight test results. This report is a prototype customer-impact report; improved versions might be provided for future File-Detection Test reports.

In this report, customer impact is measured according to prevalence. Essentially, some malware samples pose a greater threat to the average user than others, because they are more widespread. Some may target e.g. a specific company or user base, but present less of risk to the general population. Other malware samples may only be found on specific websites, affect specific countries/regions or only be relevant to particular operating system versions or interface languages.

Microsoft's initiative uses its global telemetry data (malware prevalence) to consider the customer impact posed by missed detections. That is, the malware files that antimalware products failed to detect are weighted based on malware-family prevalence, and each vendor's prevalence-weighted results are reported along with the file-detection results in this report. These results are designed to give greater insight into the customer impact of the missed detections during testing. In addition to global prevalence weighting impact, geo-location prevalence is also used to determine the customer impact of missed detections in specific countries for products tested. So, unlike a traditionally scored test which gives each sample the same weight when calculating the percent impact, samples in the prevalence-weighted model have varying impacts based on prevalence information.

This report is supplementary to AV-Comparatives' main report[1], already published, of the September 2015 File-Detection Test. No additional testing has been performed; rather, the existing test results have been re-analysed from a different perspective, to consider what impact the missed samples are likely to have on customers. It is conceivable that a product with a lower score in the test may actually protect the average user better than one with a higher score, under specific circumstances. Let us imagine that Product A detects 99% of malware samples in the test, but that the 1% of samples not detected are very widespread, and that the average user is quite likely to encounter them. Product B, on the other hand, only detects 98% of samples, but the samples missed are not as prevalent. In this case, users would probably be more at risk using Product A, as it misses more of the malware that is likely to present a threat to them. AV-Comparatives has for many years focused on using prevalent samples in its tests, as mentioned in our reports and also in a Microsoft blog[2]. Furthermore, same sample variants (e.g. polymorphic malware) are clustered into families to avoid a disproportional test-set[3]. AV-Comparatives makes uses of telemetry data from various sources, not just Microsoft, as the test-set must remain independent and not based solely on data provided by one specific vendor or organisation. Therefore, minor discrepancies between one vendor's data and our independently sorted combination are possible. The original File-Detection Test in September 2015 used a malware set sorted using various telemetry sources; however, the analysis in this supplementary report is based solely on Microsoft's data.

---

[1] http://www.av-comparatives.org/wp-content/uploads/2015/10/avc_fdt_201509_en.pdf
[2] http://blogs.technet.com/b/mmpc/archive/2010/06/15/update-on-telemetry-usage-in-tests-part-1.aspx
[3] http://blogs.technet.com/b/mmpc/archive/2009/07/16/let-telemetry-be-your-guide-a-proposal-for-security-tests.aspx

Tested products

The following products tested in September 2015 are included in this report:

- Avast Free Antivirus 10.3
- AVG Internet Security 2015.0
- AVIRA Antivirus Pro 15.0
- Baidu Antivirus 5.4.3
- Bitdefender Internet Security 18.23
- BullGuard Internet Security 15.1
- Emsisoft Anti-Malware 10.0
- eScan Internet Security 14.0
- ESET Smart Security 8.0
- F-Secure Internet Security 14.139
- Fortinet FortiClient 5.2.4
- Kaspersky Internet Security 16.0
- Lavasoft Ad-Aware Free Antivirus+ 11.8
- McAfee Internet Security 18.0
- Microsoft Windows Defender 4.8
- Panda Free Antivirus 16.0
- Quick Heal Total Security 16.0
- Sophos Endpoint Security and Control 10.3
- Tencent PC Manager 11.0
- ThreatTrack Vipre Internet Security 8.4
- Trend Micro Internet Security 10.0

The test-set used was built consulting telemetry data from various sources (not only Microsoft), with the aim of including mainly prevalent malicious samples from the last weeks/months prior the test which posed a threat to users in the field.

Detection vs. Protection

Although very important, the file-detection rate of a product is only one aspect of a complete anti-virus product. Almost all antivirus products contain features such as URL-blockers and behavioural protection that protect the user's computer without necessarily identifying every malicious file.

AV-Comparatives also provides a whole-product dynamic "real-world" protection test[4], as well as other test reports that cover these aspects/features of the products. We invite users to look at our other tests and not only the File-Detection Test, even though a good file-detection rate is still one of the most important, deterministic and reliable basic features of an anti-virus product.

[4] http://www.av-comparatives.org/dynamic-tests/

Methodology

This analysis was carried out using AV-Comparatives' file-detection test data from September 2015. Telemetry data was gathered for the files in the test over the period between June and September 2015. This telemetry came from Microsoft real-time protection (RTP) products and included not only threat telemetry but also behaviour-based early warning telemetry. This encounter rate information comes only from computers whose users have agreed to provide data to Microsoft, but includes over 200 million computers in over 100 countries and regions around the world.

Prevalence is defined as the number of distinct computers that have reported an encounter with a particular malware sample or a malware family. Distinct computers are identified through a unique product GUID (not IP address) associated with Microsoft RTP products.

To assess the prevalence-weighted impact of each sample in the test set, the following data is calculated from the ecosystem telemetry:

- The prevalence of the tested sample
- The prevalence of the malware family
- The position of that malware family relative to other malware families. A malware family can be in one of four ecosystem partitions: high, moderate, low and very low.

Ecosystem Partition Weight Calculation

To calculate the ecosystem partition weight, all eligible families are identified from ecosystem telemetry over the test set time period. Eligible families are those that have high or severe impact to a customer and are not disputable families. Disputable families are those that are considered to be "potentially unwanted" (such as adware or bundled software). The customer impact of each family is calculated by measuring the number of computers reporting that malware family (prevalence), and then the families are ranked by impact from highest to lowest prevalence. The families are divided into partitions: high, moderate, low and very low using the Head Tail breaks method[5]. Then, the prevalence of each partition is calculated. So, if families in the high partition represent 80% of the ecosystem malware encountered, the test-set families in high will account for 80% of the test score.

[5] https://en.wikipedia.org/wiki/Head/tail_Breaks

Family Weight Calculation

Next, the family weight of the test set families is calculated by dividing the prevalence of the family by the ecosystem prevalence of all families in the test set. So, if a family was encountered by 1,000 computers in the ecosystem and the total number of computer malware family encounters in the test set was 1,000,000, then the family weight would be 0.1%

If a family is in the high or moderate partition and has less than 50 samples in the test set, then the family weight is multiplied by the number of samples in the test set divided by 50. For example, if the family weight of a high family was 0.1%, but there were only 25 samples in the test set, then the family weight would be adjusted to 0.05% to account for the small sample set representing that family.

Some malware families are not true families that represent malware of a common origin, but instead are heuristic methods of detecting malware. These types of "families" are called generic families. Malware detected by Microsoft's generic signatures could be members of classified or unclassified "real" families. Most prevalent samples are categorized into their true family using Microsoft detection names[6] or AV-Comparatives family mapping. However, some samples will still fall into generic family categories. Therefore, any samples that are detected with a generic family are given a family weight equal to the average of all real family weights. In the case that a sample was a member of a family that had no prevalence information in the Microsoft ecosystem or that was not detected by Microsoft during that timeframe, it will also receive the average family for this calculation.

Descriptions and information about malware families can be found in the Microsoft Malware Protection Center's Malware Encyclopedia http://www.microsoft.com/security/portal/threat/Threats.aspx

Family Impact to Test Set (Partition-adjusted family weight)

After the partition and family weights are calculated, the families are normalized by their partition by dividing the family weight by the sum of all family weights in that family's partition, and then by multiplying the result by the partition percent. This normalization ensures that the family weights closely match the ecosystem. For example, if the family represented 0.1% of the partition, and the family's partition represents 50% of the test set, then the partition-adjusted family weight is 0.05% which represents that family's total impact to the test set.

Sample Impact to Test Set

The next step is to calculate the prevalence of each sample, which is used to establish that sample's importance respective to other samples in the same malware family. This step is calculated by dividing the prevalence of each file by the prevalence of all files in that family. For example, let's say there are 91 samples in a family. 90 of them were encountered by only 1 computer, but one sample was encountered by 10 computers. The one sample affecting 10 computers would account for 10% (10 / (90+10)) of that family's impact and the remaining samples would each account for 1%.

[6] http://www.microsoft.com/security/portal/mmpc/shared/malwarenaming.aspx

After calculating the sample's impact to the family, the final sample impact to the test set is calculated by multiplying the sample impact to the family with the partition adjusted family weight. For example, if the sample represented 10% of the family, and the partition adjusted family weight was 0.05%, the sample's test impact is 0.005% (10% * 0.05%) and the remaining 90 samples represent 0.045%.

Vendor Test Score Calculation

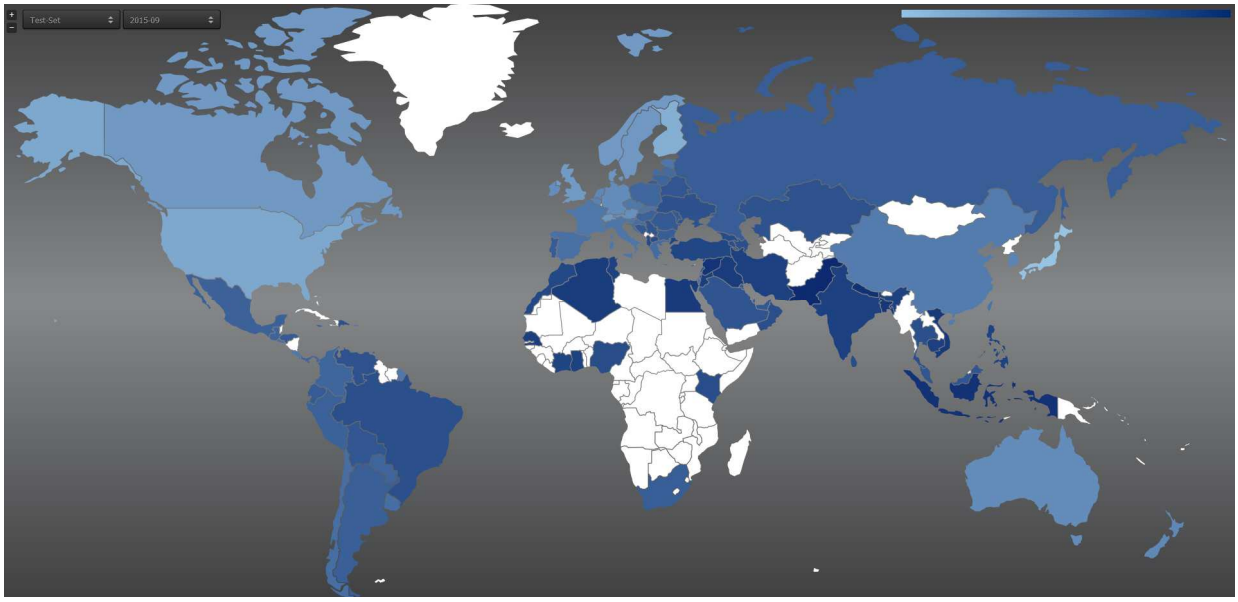
Each vendor's test score is created by subtracting the sum of the impact of all missed samples from 1. So, if the vendor only missed the one sample impacting 10 computers in the example above, then the vendor's prevalence-weighted test score would be 99.995%.

Country Vendor Test Score Calculation

A vendor test score is calculated for any region that had 10,000 or more computers reporting threats during the test set period. The calculation works exactly the same as the worldwide calculation. However, the prevalence information used to calculate the partition-adjusted family weight comes solely from that country rather than the worldwide telemetry to highlight the vendor's protection against the most prevalent threats affecting that particular locale.

Test-Set description

The test-set used in September 2015 for the File-Detection Test contained 166522 malware samples. The number of encounters caused by the malware samples used in the test was according to Microsoft's telemetry data around 3,568,492. The malware families represented by the test set had nearly 40 million computer encounters. The world map below shows the countries in which these malware families had the biggest impact.



There are over 150 countries of the world for which Microsoft have data for less than 10,000 computers reporting threats. These are considered to be too small to be statistically relevant – the margin of error is too high to accurately represent the population of Internet users in the country. These appear as white on the map. The impact on the remaining ~100 countries are shown as blue in the map.

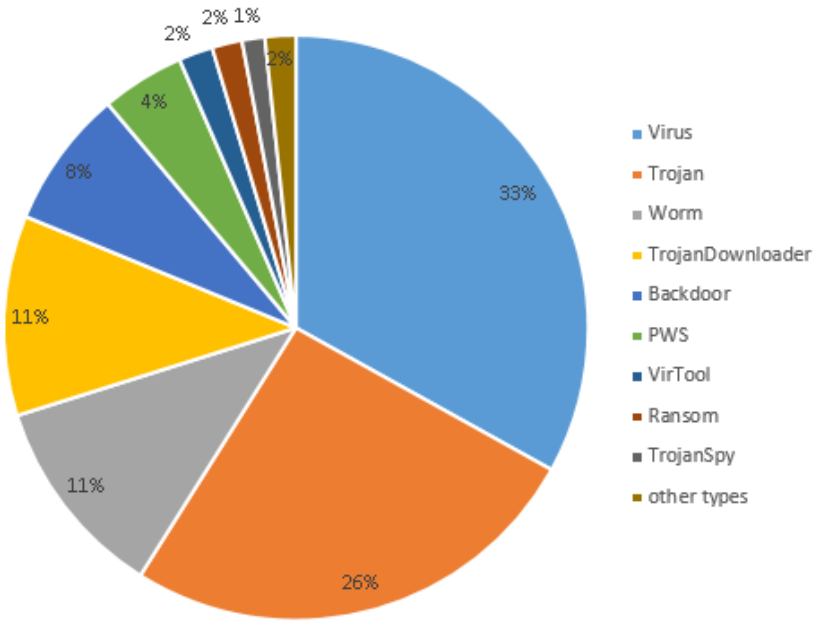
Top 15 most impacted countries:

1.	Pakistan	38.8%
2.	Nepal	34.7%
3.	Palestina	33.9%
4.	Indonesia	33.7%
5.	Syria	32.8%
6.	Bangladesh	30.9%
7.	Vietnam	30.3%
8.	Egypt	29.0%
9.	Algeria	28.8%
10.	Iraq	28.6%
11.	Jordan	27.8%
12.	Senegal	27.4%
13.	Cambodia	27.0%
14.	India	26.3%
15.	Iran	26.2%

Top 15 less impacted countries:

1.	Japan	2.3%
2.	Finland	3.4%
3.	United States	3.8%
4.	United Kingdom	4.9%
5.	Norway	4.9%
6.	Canada	5.0%
7.	Sweden	5.1%
8.	Switzerland	5.3%
9.	Denmark	5.4%
10.	Austria	5.9%
11.	Ireland	6.2%
12.	Germany	6.4%
13.	Australia	6.4%
14.	Hong Kong	6.7%
15.	Netherlands	6.9%

Distribution of Malware Types in the test-set



Top 20 Malware Families in the test-set (partitions in parenthesis)

1. Sality	10.6% (High)	11. Vobfus	3.1% (Moderate)
2. Virut	10.4% (High)	12. Bagsu	2.0% (Very Low)
3. Upatre	7.3% (Moderate)	13. Kovter	1.7% (Moderate)
4. Dynamer	6.2% (Very Low)	14. Parite	1.5% (Low)
5. Blakamba	6.1% (High)	15. Fynloski	1.2% (Moderate)
6. Skeeyah	5.7% (Very Low)	16. Dorv	1.2% (Moderate)
7. Bladabindi	4.3% (Moderate)	17. Mytonel	1.0% (Moderate)
8. Gamarue	3.8% (High)	18. Nitol	0.9% (Moderate)
9. ZBot	3.7% (Moderate)	19. Nabacur	0.9% (Very Low)
10. Ramnit	3.5% (High)	20. Brontok	0.8% (Moderate)

Top 10 Test Set Malware Families[7] with highest encounter rates in Microsoft's ecosystem

Malware Family	Ecosystem Computers
1. Peals	4010584
2. Skeeyah	3922232
3. Obfuscator	3042352
4. Gamarue	2668591
5. Blakamba	1919280
6. Jenxcus	1536779
7. Dorv	1448727
8. Sventore	1421714
9. Autorun	1348608
10. Dynamer	1269807

Top 10 Test Set Malware Families with highest Test Impact

Malware Family	Test Impact
1. Gamarue	16.8%
2. Blakamba	12.1%
3. Dorv	9.1%
4. Ramnit	5.2%
5. Jenxcus	5.2%
6. Sality	5.1%
7. Virut	2.7%
8. Bladabindi	2.5%
9. Nuqel	1.5%
10. Brontok	1.5%

[7] The families in bold are generic family names and therefore carry a very low test impact even if they are encountered relatively often.

Detection Rates and Customer Impact

Based on the missed samples and the detection rate over the whole test-set, Microsoft have calculated the Prevalence-Weighted Test Score. This can be seen in the table below.

	Prevalence-Weighted Test Score	Missed Samples	*100% -Missed Samples*	*Difference in Scores*
1. AVIRA	99.7%	0.2%	*99.8%*	*-0.1%*
2. Baidu	99.5%	0.6%	*99.4%*	*+0.1%*
3. F-Secure	99.5%	0.3%	*99.7%*	*-0.2%*
4. ESET	99.4%	0.8%	*99.2%*	*+0.2%*
5. Panda	99.3%	1.4%	*98.6%*	*+0.7%*
6. Microsoft	99.0%	8.6%	*91.4%*	*+7.6%*
7. ThreatTrack	98.9%	1.8%	*98.2%*	*+0.7%*
8. Kaspersky Lab	98.9%	0.5%	*99.5%*	*-0.6%*
9. Emsisoft	98.8%	0.3%	*99.7%*	*-0.9%*
10. Bitdefender	98.7%	0.2%	*99.8%*	*-1.1%*
11. Fortinet	98.6%	1.2%	*98.8%*	*-0.2%*
12. Lavasoft	98.3%	0.3%	*99.7%*	*-1.4%*
13. BullGuard	98.3%	0.3%	*99.7%*	*-1.4%*
14. Quick Heal	98.3%	0.3%	*99.7%*	*-1.4%*
15. eScan	98.3%	0.3%	*99.7%*	*-1.4%*
16. Trend Micro	98.2%	4.5%	*95.5%*	*+2.7%*
17. McAfee	98.0%	2.5%	*97.5%*	*+0.5%*
18. Sophos	98.0%	2.8%	*97.2%*	*+0.8%*
19. Tencent	96.2%	2.6%	*97.4%*	*-1.2%*
20. Avast	95.9%	0.8%	*99.2%*	*-3.3%*
21. AVG	89.3%	6.6%	*93.4%*	*-4.1%*

Heat-Maps Overview

The interactive heat maps for all countries can be found on http://impact.av-comparatives.org

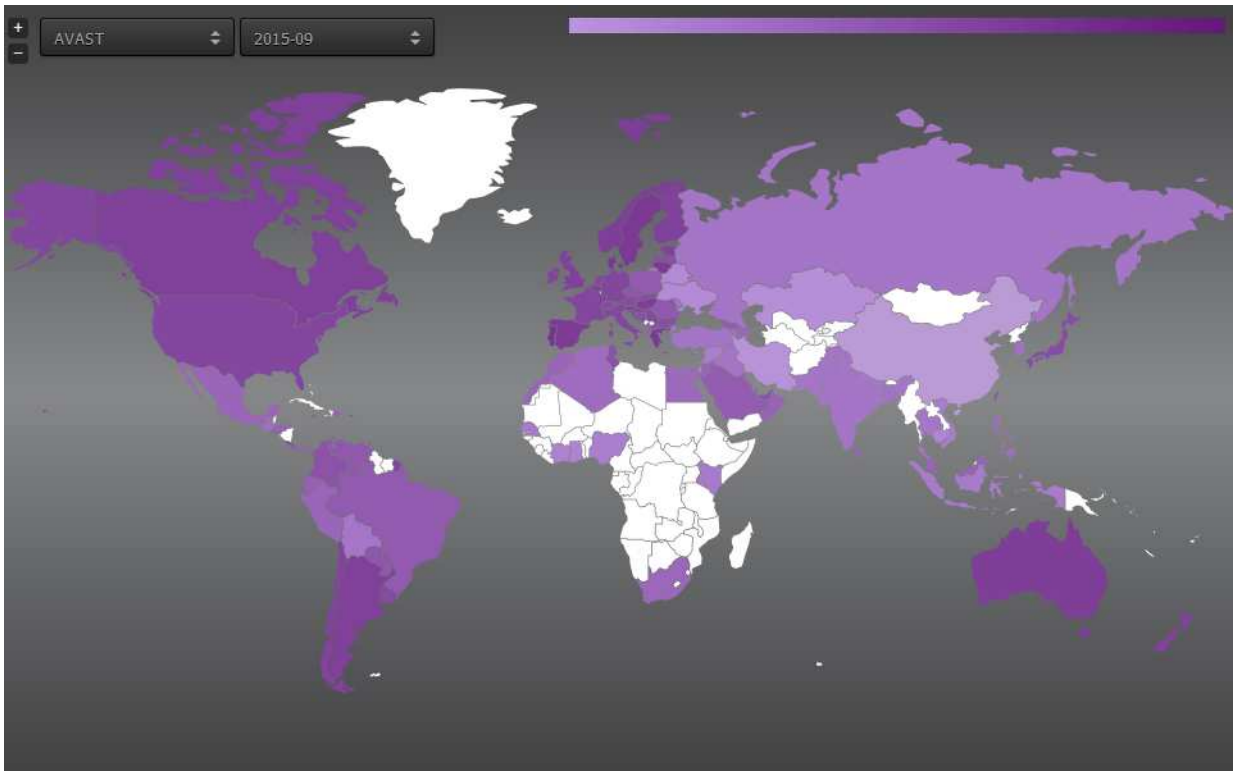
The heat maps for each vendor, i.e. the coloured maps of the world show data that is normalised by the relative size of the country. Thus the maps represent the countries with the highest risk relative to the prevalence of files that were missed in the test set. This normalisation differs from the heat map displayed in the **Test-Set Description** (on page 7); that map is normalised based on the prevalence of the entire test set to show the prevalence of the files that were used in the test set. As a consequence, the scale on the vendor-specific heat maps and the colours shows are not directly comparable to the test-set description heat map.

The table below shows the numbers only for the largest markets according to the Microsoft data, i.e. only for the countries where Microsoft saw more than 5 million reporting machines.

	Australia	Brazil	Canada	China	France	Germany	India	Italy	Japan	Mexico	Netherlands	Russia	Spain	UK	USA
Avira	99,1%	99,7%	99,2%	100,0%	99,3%	99,3%	99,9%	99,4%	99,5%	99,8%	99,4%	99,9%	99,1%	99,2%	99,3%
Baidu	98,7%	99,6%	98,9%	99,9%	99,1%	99,1%	99,7%	99,1%	99,2%	99,6%	99,1%	99,7%	98,8%	98,9%	99,1%
F-Secure	99,2%	99,3%	99,3%	99,8%	99,4%	99,3%	99,6%	99,4%	99,5%	99,3%	99,3%	99,8%	99,2%	99,3%	99,4%
ESET	99,0%	98,7%	99,1%	98,5%	99,2%	98,8%	99,7%	99,2%	99,2%	99,7%	98,9%	99,3%	99,0%	99,1%	99,2%
Panda	99,4%	99,4%	99,4%	98,5%	99,5%	99,3%	99,5%	99,5%	99,4%	99,2%	99,4%	99,6%	99,1%	99,5%	99,5%
Microsoft	99,0%	98,9%	98,8%	98,4%	98,8%	98,7%	99,2%	99,0%	99,1%	98,9%	98,5%	99,0%	99,1%	99,0%	99,0%
ThreatTrack	99,5%	99,3%	99,5%	97,5%	99,5%	99,1%	99,1%	99,3%	99,3%	99,0%	99,0%	98,5%	99,4%	99,5%	99,6%
Kaspersky Lab	97,2%	98,3%	97,3%	99,8%	97,0%	97,4%	99,5%	97,7%	97,4%	99,3%	97,6%	98,9%	97,3%	97,1%	97,0%
Emsisoft	98,3%	97,7%	98,2%	99,4%	97,8%	98,0%	99,1%	98,3%	98,0%	98,6%	98,4%	98,9%	98,4%	98,1%	97,8%
Bitdefender	98,1%	97,3%	97,8%	99,5%	96,7%	97,3%	99,3%	97,9%	97,0%	99,0%	98,0%	98,3%	98,4%	97,4%	96,7%
Fortinet	97,4%	98,5%	97,6%	98,5%	97,9%	97,9%	98,9%	98,0%	98,1%	98,4%	97,8%	99,3%	97,2%	97,6%	98,0%
Lavasoft	97,3%	96,6%	97,2%	99,3%	96,1%	96,8%	98,9%	97,3%	96,5%	98,4%	97,4%	98,1%	97,6%	96,7%	96,1%
BullGuard	97,3%	96,6%	97,2%	99,3%	96,1%	96,8%	98,9%	97,3%	96,5%	98,4%	97,4%	98,1%	97,6%	96,7%	96,1%
Quick Heal	97,3%	96,6%	97,2%	99,4%	96,1%	96,8%	98,9%	97,3%	96,5%	98,3%	97,4%	98,1%	97,6%	96,7%	96,1%
eScan	97,3%	96,6%	97,2%	99,3%	96,1%	96,8%	98,9%	97,3%	96,5%	98,3%	97,4%	98,1%	97,6%	96,7%	96,1%
Trend Micro	96,8%	98,5%	96,8%	98,2%	97,4%	97,2%	98,8%	97,3%	96,7%	98,6%	97,3%	98,1%	96,6%	96,8%	97,2%
McAfee	95,8%	97,9%	95,2%	98,6%	96,1%	96,1%	98,9%	96,3%	97,2%	98,3%	96,8%	99,1%	95,5%	96,1%	96,2%
Sophos	97,4%	97,3%	97,2%	97,0%	96,9%	96,9%	98,6%	97,4%	96,5%	98,2%	97,3%	97,4%	97,3%	97,1%	96,9%
Tencent	95,0%	97,8%	95,3%	97,5%	96,3%	95,1%	96,2%	95,1%	96,4%	94,9%	95,7%	95,2%	95,0%	95,5%	96,1%
Avast	87,7%	95,1%	88,8%	99,3%	90,7%	90,7%	98,0%	90,9%	92,2%	96,7%	90,9%	98,0%	87,1%	89,0%	90,6%
AVG	66,8%	87,3%	69,8%	98,9%	74,9%	74,8%	95,5%	75,8%	78,9%	92,6%	74,8%	94,7%	65,5%	70,6%	74,7%

Avast

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:



Customer Impact by Country/Region (normalised):

1. Portugal	17388 in 100000	11. Puerto Rico	11644 in 100000
2. Denmark	15465 in 100000	12. Belgium	11352 in 100000
3. Greece	14323 in 100000	13. **Canada**	11152 in 100000
4. Sweden	14037 in 100000	14. Argentina	11057 in 100000
5. Lithuania	13318 in 100000	15. Estonia	10961 in 100000
6. Slovenia	13255 in 100000	16. **United Kingdom**	10960 in 100000
7. **Spain**	12908 in 100000	17. Finland	10950 in 100000
8. **Australia**	12339 in 100000	18. Reunion	10838 in 100000
9. Norway	11954 in 100000	19. New Zealand	10436 in 100000
10. Hungary	11794 in 100000	20. Ireland	10111 in 100000

Global Non-Detection Risk: 4149 in 100000

Top 5 missed malware families:
1. Blakamba
2. Jenxcus
3. Gamarue
4. Bladabindi
5. Ogimant

AVG

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Portugal	46066 in 100000	11. Belgium	30955 in 100000
2. Denmark	41574 in 100000	12. **Canada**	30164 in 100000
3. Greece	38462 in 100000	13. Puerto Rico	29966 in 100000
4. Sweden	38122 in 100000	14. Finland	29859 in 100000
5. Slovenia	36444 in 100000	15. **United Kingdom**	29378 in 100000
6. Lithuania	35637 in 100000	16. Estonia	29353 in 100000
7. **Spain**	34509 in 100000	17. Reunion	29103 in 100000
8. **Australia**	33167 in 100000	18. New Zealand	28185 in 100000
9. Norway	32556 in 100000	19. Argentina	27872 in 100000
10. Hungary	32093 in 100000	20. Ireland	27778 in 100000

Global Non-Detection Risk: 10665 in 100000

Top 5 missed malware families:
1. Blakamba
2. Kilim
3. Jenxcus
4. Spallowz
5. Bladabindi

AVIRA

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Portugal	1209 in 100000	11. **Canada**	803 in 100000
2. Denmark	1086 in 100000	12. Belgium	785 in 100000
3. Greece	999 in 100000	13. Finland	775 in 100000
4. Sweden	984 in 100000	14. Puerto Rico	770 in 100000
5. Lithuania	931 in 100000	15. **United Kingdom**	767 in 100000
6. Slovenia	923 in 100000	16. Estonia	762 in 100000
7. **Spain**	901 in 100000	17. Reunion	761 in 100000
8. **Australia**	862 in 100000	18. New Zealand	731 in 100000
9. Norway	848 in 100000	19. Argentina	717 in 100000
10. Hungary	822 in 100000	20. Ireland	704 in 100000

Global Non-Detection Risk: 262 in 100000

Top 5 missed malware families:
1. Blakamba
2. Dacic
3. Fincomp
4. Virut
5. Anaki

Baidu (International/English version)

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Portugal	1636 in 100000	11. **Canada**	1118 in 100000
2. Denmark	1478 in 100000	12. **United Kingdom**	1089 in 100000
3. Greece	1374 in 100000	13. Belgium	1084 in 100000
4. Sweden	1349 in 100000	14. Estonia	1079 in 100000
5. Lithuania	1275 in 100000	15. Ireland	1078 in 100000
6. Slovenia	1273 in 100000	16. Finland	1063 in 100000
7. **Australia**	1250 in 100000	17. New Zealand	1055 in 100000
8. **Spain**	1237 in 100000	18. Puerto Rico	1040 in 100000
9. Norway	1157 in 100000	19. Reunion	1035 in 100000
10. Hungary	1131 in 100000	20. Argentina	968 in 100000

Global Non-Detection Risk: 458 in 100000

Top 5 missed malware families:
1. Blakamba
2. Gamarue
3. Upatre
4. Bladabindi
5. Zbot

Bitdefender

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. **France**	3346 in 100000	11. **Canada**	2159 in 100000
2. **United States**	3328 in 100000	12. Chile	2155 in 100000
3. **Japan**	3035 in 100000	13. Paraguay	2114 in 100000
4. Poland	2952 in 100000	14. **Italy**	2110 in 100000
5. **Brazil**	2737 in 100000	15. Argentina	2089 in 100000
6. **Germany**	2654 in 100000	16. Switzerland	2072 in 100000
7. **United Kingdom**	2634 in 100000	17. **Netherlands**	2026 in 100000
8. Norway	2280 in 100000	18. Belgium	1975 in 100000
9. Finland	2275 in 100000	19. New Zealand	1975 in 100000
10. Israel	2265 in 100000	20. **Australia**	1940 in 100000

Global Non-Detection Risk: 1296 in 100000

Top 5 missed malware families:

1. Dorv
2. Jenxcus
3. Diztakun
4. Fareit
5. Regiskazi

BullGuard

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. **France**	3944 in 100000	11. Norway	2999 in 100000
2. **United States**	3884 in 100000	12. Finland	2962 in 100000
3. Paraguay	3729 in 100000	13. **Canada**	2836 in 100000
4. **Japan**	3536 in 100000	14. Trinidad a. Tobago	2773 in 100000
5. **Brazil**	3446 in 100000	15. Belgium	2696 in 100000
6. Poland	3292 in 100000	16. **Australia**	2689 in 100000
7. **United Kingdom**	3275 in 100000	17. **Italy**	2683 in 100000
8. **Germany**	3206 in 100000	18. Israel	2678 in 100000
9. Chile	3199 in 100000	19. New Zealand	2632 in 100000
10. Argentina	3086 in 100000	20. Tunisia	2625 in 100000

Global Non-Detection Risk: 1702 in 100000

Top 5 missed malware families:

1. Dorv
2. Jenxcus
3. Blakamba
4. Diztakun
5. Bladabindi

Emsisoft

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Paraguay	3486 in 100000	11. Panama	2106 in 100000
2. Chile	2391 in 100000	12. Puerto Rico	2014 in 100000
3. Tunisia	2361 in 100000	13. **Japan**	2000 in 100000
4. Colombia	2345 in 100000	14. **Germany**	1963 in 100000
5. **Brazil**	2277 in 100000	15. Jamaica	1957 in 100000
6. Venezuela	2265 in 100000	16. **United Kingdom**	1939 in 100000
7. Argentina	2264 in 100000	17. Norway	1911 in 100000
8. **France**	2248 in 100000	18. Costa Rica	1910 in 100000
9. Trinidad and Tobago	2191 in 100000	19. Finland	1902 in 100000
10. **United States**	2159 in 100000	20. Poland	1802 in 100000

Global Non-Detection Risk: 1185 in 100000

Top 5 missed malware families:

1. Dorv
2. Jenxcus
3. Blakamba
4. Diztakun
5. Bladabindi

eScan

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. **France**	4818 in 100000	11. Norway	3304 in 100000
2. **United States**	4620 in 100000	12. Finland	2923 in 100000
3. Paraguay	4319 in 100000	13. **Canada**	2760 in 100000
4. **Japan**	4268 in 100000	14. Trinidad and Tobago	2744 in 100000
5. **Brazil**	4206 in 100000	15. Belgium	2718 in 100000
6. Poland	3839 in 100000	16. **Australia**	2698 in 100000
7. **United Kingdom**	3701 in 100000	17. **Italy**	2644 in 100000
8. **Germany**	3514 in 100000	18. Israel	2628 in 100000
9. Chile	3512 in 100000	19. Tunisia	2626 in 100000
10. Argentina	3493 in 100000	20. New Zealand	2625 in 100000

Global Non-Detection Risk: 1722 in 100000

Top 5 missed malware families:

1. Dorv
2. Jenxcus
3. Blakamba
4. Diztakun
5. Bladabindi

ESET

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Macedonia	1750 in 100000	11. Greece	1200 in 100000
2. Bosnia and Herzegovina	1614 in 100000	12. **Germany**	1191 in 100000
3. Albania	1598 in 100000	13. Lithuania	1169 in 100000
4. Serbia	1583 in 100000	14. Sweden	1158 in 100000
5. **China**	1541 in 100000	15. Slovenia	1151 in 100000
6. Hong Kong	1404 in 100000	16. Finland	1150 in 100000
7. **Brazil**	1326 in 100000	17. Norway	1104 in 100000
8. Croatia	1317 in 100000	18. **Netherlands**	1063 in 100000
9. Denmark	1203 in 100000	19. Reunion	1037 in 100000
10. Portugal	1200 in 100000	20. **Spain**	1034 in 100000

Global Non-Detection Risk: 599 in 100000

Top 5 missed malware families:
1. Blakamba
2. Diztakun
3. Helompy
4. Tembatch
5. Noancooe

F-Secure

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Paraguay	1706 in 100000	11. Jamaica	997 in 100000
2. Tunisia	1219 in 100000	12. Denmark	980 in 100000
3. Colombia	1218 in 100000	13. Slovenia	978 in 100000
4. Puerto Rico	1160 in 100000	14. Greece	925 in 100000
5. Venezuela	1133 in 100000	15. Sweden	910 in 100000
6. Trinidad and Tobago	1124 in 100000	16. Lithuania	904 in 100000
7. Chile	1116 in 100000	17. Reunion	885 in 100000
8. Portugal	1054 in 100000	18. Saudi Arabia	865 in 100000
9. Argentina	1051 in 100000	19. Slovak Republic	833 in 100000
10. Panama	997 in 100000	20. **Spain**	825 in 100000

Global Non-Detection Risk: 470 in 100000

Top 5 missed malware families:
1. Blakamba
2. Jenxcus
3. Bladabindi
4. Rootkit
5. Mogoogwi

Fortinet

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Taiwan	6765 in 100000	11. **Spain**	2804 in 100000
2. Slovenia	3695 in 100000	12. Bosnia and Herzegovina	2727 in 100000
3. Portugal	3571 in 100000	13. Croatia	2685 in 100000
4. Denmark	3278 in 100000	14. Macedonia	2678 in 100000
5. Greece	3205 in 100000	15. Norway	2671 in 100000
6. Sweden	3058 in 100000	16. **Australia**	2603 in 100000
7. Egypt	2994 in 100000	17. Finland	2573 in 100000
8. Hungary	2979 in 100000	18. Belgium	3543 in 100000
9. Serbia	3958 in 100000	19. New Zealand	2541 in 100000
10. Lithuania	2880 in 100000	20. Reunion	3630 in 100000

Global Non-Detection Risk: 1412 in 100000

Top 5 missed malware families:
1. Blakamba
2. Nuqel
3. Ramnit
4. Sohanad
5. Helompy

Kaspersky Lab

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

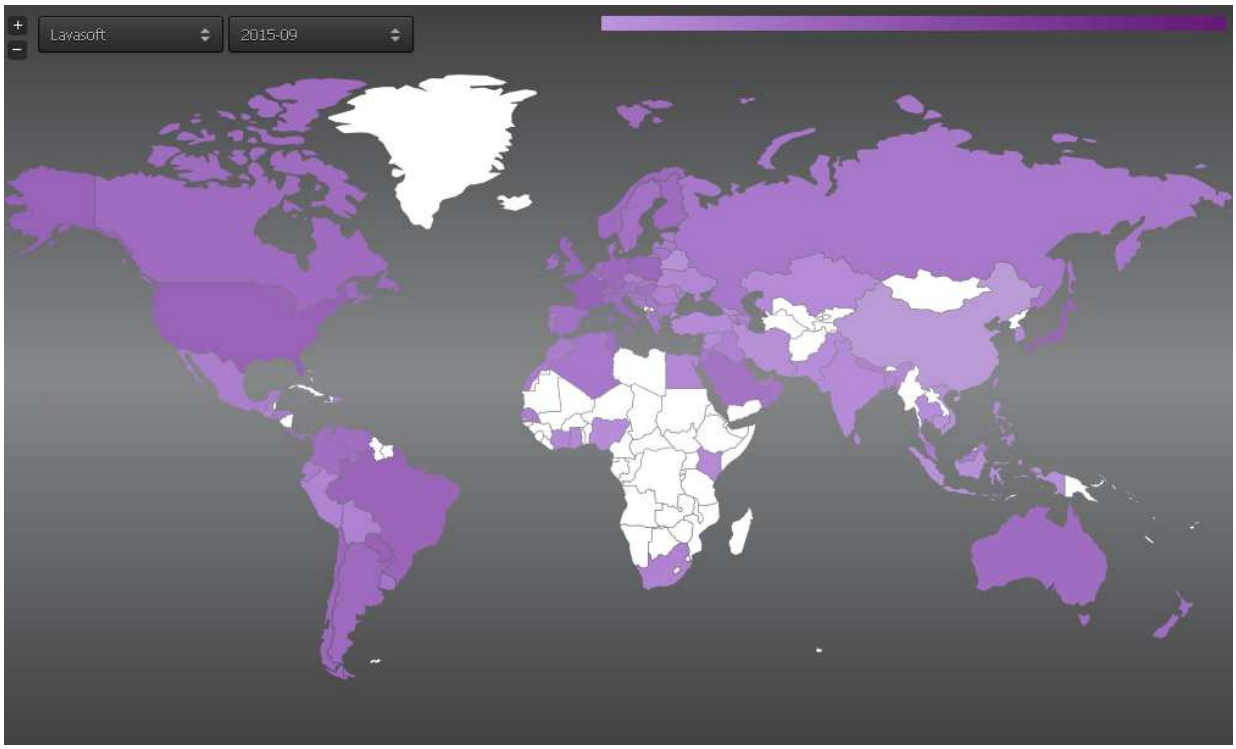
1. Denmark	3091 in 100000	11. **Canada**	2713 in 100000
2. Portugal	3076 in 100000	12. Lithuania	2690 in 100000
3. **United States**	2974 in 100000	13. Belgium	2679 in 100000
4. **France**	2965 in 100000	14. Greece	2670 in 100000
5. Norway	2958 in 100000	15. Hungary	2652 in 100000
6. Sweden	2953 in 100000	16. New Zealand	2637 in 100000
7. **United Kingdom**	2894 in 100000	17. **Japan**	2614 in 100000
8. Finland	2868 in 100000	18. **Germany**	2603 in 100000
9. **Australia**	2830 in 100000	19. Slovenia	2575 in 100000
10. **Spain**	2729 in 100000	20. Ireland	2491 in 100000

Global Non-Detection Risk: 1061 in 100000

Top 5 missed malware families:
1. Blakamba
2. Dorv
3. Asemload
4. Wesonten
5. Startpage

Lavasoft

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:



Customer Impact by Country/Region (normalised):

1. **France**	3940 in 100000	11. Norway	2999 in 100000
2. **United States**	3884 in 100000	12. Finland	2962 in 100000
3. Paraguay	3729 in 100000	13. **Canada**	2836 in 100000
4. **Japan**	3536 in 100000	14. Trinidad and Tobago	2773 in 100000
5. **Brazil**	3446 in 100000	15. Belgium	2696 in 100000
6. Poland	3292 in 100000	16. **Australia**	2689 in 100000
7. **United Kingdom**	3275 in 100000	17. **Italy**	2683 in 100000
8. **Germany**	3206 in 100000	18. Israel	2678 in 100000
9. Chile	3199 in 100000	19. New Zealand	2632 in 100000
10. Argentina	3086 in 100000	20. Tunisia	2625 in 100000

Global Non-Detection Risk: 1702 in 100000

Top 5 missed malware families:

1. Dorv
2. Jenxcus
3. Blakamba
4. Diztakun
5. Bladabindi

McAfee / Intel Security

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Portugal	5503 in 100000	11. Puerto Rico	4184 in 100000
2. Denmark	5153 in 100000	12. **France**	3949 in 100000
3. **Canada**	4784 in 100000	13. **United Kingdom**	3887 in 100000
4. Greece	4704 in 100000	14. **Germany**	3868 in 100000
5. Sweden	4699 in 100000	15. Hungary	3857 in 100000
6. **Spain**	4549 in 100000	16. Argentina	3836 in 100000
7. Slovenia	4412 in 100000	17. Finland	3818 in 100000
8. Lithuania	4364 in 100000	18. Reunion	3806 in 100000
9. Norway	4265 in 100000	19. Belgium	3788 in 100000
10. **Australia**	4213 in 100000	20. **United States**	3775 in 100000

Global Non-Detection Risk: 1965 in 100000

Top 5 missed malware families:

1. Blakamba
2. Dacic
3. Jenxcus
4. Gamarue
5. Ramnit

Microsoft

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Malaysia	2836 in 100000	11. Israel	1776 in 100000
2. Paraguay	2804 in 100000	12. Romania	1774 in 100000
3. Taiwan	2302 in 100000	13. Venezuela	1754 in 100000
4. Kazakhstan	2061 in 100000	14. Bahrain	1729 in 100000
5. Tunisia	1998 in 100000	15. Kuwait	1708 in 100000
6. Panama	1988 in 100000	16. Senegal	1704 in 100000
7. Trinidad and Tobago	1977 in 100000	17. Bolivia	1689 in 100000
8. Egypt	1906 in 100000	18. Slovak Republic	1683 in 100000
9. Algeria	1839 in 100000	19. Costa Rica	1674 in 100000
10. Reunion	1797 in 100000	20. Czech Republic	1670 in 100000

Global Non-Detection Risk: 1038 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Noancooe
3. Dorv
4. Dacic
5. Bladabindi

Panda

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Cote d'Ivoire	2421 in 100000	11. Ghana	1173 in 100000
2. Morocco	1866 in 100000	12. Colombia	1130 in 100000
3. Peru	1581 in 100000	13. Albania	1056 in 100000
4. **China**	1463 in 100000	14. Ecuador	989 in 100000
5. Nepal	1370 in 100000	15. Nigeria	988 in 100000
6. Algeria	1345 in 100000	16. Uruguay	936 in 100000
7. Senegal	1345 in 100000	17. **Spain**	898 in 100000
8. Honduras	1298 in 100000	18. Costa Rica	856 in 100000
9. Indonesia	1271 in 100000	19. Argentina	828 in 100000
10. Philippines	1196 in 100000	20. **Mexico**	816 in 100000

Global Non-Detection Risk: 712 in 100000

Top 5 missed malware families:
1. Yeltminky
2. Ramnit
3. Blakamba
4. Diztakun
5. Nuqel

Quick Heal (Total Security)

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. **France**	3942 in 100000	11. Norway	2994 in 100000
2. **United States**	3878 in 100000	12. Finland	2959 in 100000
3. Paraguay	3717 in 100000	13. **Canada**	2822 in 100000
4. **Japan**	3506 in 100000	14. Trinidad and Tobago	2769 in 100000
5. **Brazil**	3435 in 100000	15. Belgium	2693 in 100000
6. Poland	3288 in 100000	16. **Italy**	2678 in 100000
7. **United Kingdom**	3271 in 100000	17. **Australia**	2677 in 100000
8. **Germany**	3201 in 100000	18. Israel	2666 in 100000
9. Chile	3194 in 100000	19. Tunisia	2644 in 100000
10. Argentina	3074 in 100000	20. New Zealand	2619 in 100000

Global Non-Detection Risk: 1705 in 100000

Top 5 missed malware families:

1. Dorv
2. Jenxcus
3. Blakamba
4. Diztakun
5. Bladabindi

Sophos

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Slovenia	3644 in 100000	11. Austria	2900 in 100000
2. **Japan**	3454 in 100000	12. Norway	2880 in 100000
3. **Germany**	3120 in 100000	13. Poland	2829 in 100000
4. **United States**	2116 in 100000	14. **Canada**	2755 in 100000
5. Hungary	3115 in 100000	15. **Spain**	2746 in 100000
6. **France**	3061 in 100000	16. Chile	2693 in 100000
7. Cote D'Ivoire	3018 in 100000	17. Latvia	2689 in 100000
8. **China**	3008 in 100000	18. Argentina	2687 in 100000
9. Finland	2989 in 100000	19. Paraguay	2681 in 100000
10. **United Kingdom**	2941 in 100000	20. Venezuela	2666 in 100000

Global Non-Detection Risk: 2015 in 100000

Top 5 missed malware families:

1. Dorv
2. Blakamba
3. Gamarue
4. Jenxcus
5. Ramnit

Tencent (International/English version)

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Bulgaria	7276 in 100000	11. Ecuador	5734 in 100000
2. Portugal	6753 in 100000	12. Peru	5638 in 100000
3. Ukraine	3144 in 100000	13. Sweden	5601 in 100000
4. Denmark	6106 in 100000	14. Macedonia	5486 in 100000
5. Greece	6096 in 100000	15. Croatia	5289 in 100000
6. Belarus	6016 in 100000	16. Guatemala	5280 in 100000
7. Bolivia	5953 in 100000	17. Serbia	5182 in 100000
8. Estonia	5870 in 100000	18. El Salvador	5127 in 100000
9. Lithuania	5857 in 100000	19. **Mexico**	5126 in 100000
10. Slovenia	5753 in 100000	20. Honduras	5070 in 100000

Global Non-Detection Risk: 3812 in 100000

Top 5 missed malware families:
1. Gamarue
2. Blakamba
3. Torwofun
4. Tarcloin
5. Bladabindi

ThreatTrack Vipre

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Cote d'Ivoire	4571 in 100000	11. **Russian Federation**	1529 in 100000
2. Senegal	2840 in 100000	12. Azerbaijan	1526 in 100000
3. **China**	2537 in 100000	13. Ukraine	1523 in 100000
4. Ghana	2341 in 100000	14. Poland	1435 in 100000
5. Taiwan	1715 in 100000	15. Moldova	1430 in 100000
6. Belarus	1667 in 100000	16. Slovenia	1388 in 100000
7. Turkey	1624 in 100000	17. Algeria	1373 in 100000
8. Kazakhstan	1615 in 100000	18. Bolivia	1342 in 100000
9. Armenia	1541 in 100000	19. Czech Republic	1328 in 100000
10. Korea (south)	1540 in 100000	20. Cambodia	1320 in 100000

Global Non-Detection Risk: 1053 in 100000

Top 5 missed malware families:
1. Gamarue
2. Ramnit
3. Spallowz
4. Ogimant
5. Macoute

Trend Micro

The world map below shows the encounter rates across the globe based on the distribution of samples missed by this vendor:

Customer Impact by Country/Region (normalised):

1. Portugal	4030 in 100000	11. Estonia	3233 in 100000
2. Sri Lanka	4002 in 100000	12. **Australia**	2309 in 100000
3. Denmark	3758 in 100000	13. **United Kingdom**	2195 in 100000
4. Greece	3514 in 100000	14. Norway	3168 in 100000
5. Sweden	3492 in 100000	15. Hungary	3056 in 100000
6. **Spain**	3449 in 100000	16. Finland	3019 in 100000
7. Lithuania	3427 in 100000	17. Austria	2986 in 100000
8. Slovenia	3290 in 100000	18. Belgium	2935 in 100000
9. **Japan**	3265 in 100000	19. New Zealand	2828 in 100000
10. **Canada**	3237 in 100000	20. **United States**	2828 in 100000

Global Non-Detection Risk: 1782 in 100000

Top 5 missed malware families:
1. Blakamba
2. Gamarue
3. Dorv
4. Ramnit
5. Kovter

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives (November 2015)