Addendum to the File Detection Test of March 2016

Language: English
March 2016
Last Revision: 25th April 2016

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 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 March 2016 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 March 2016 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/2016/04/avc_fdt_201603_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 March 2016 are included in this report:

- Avast Free Antivirus 11.1
- AVG Internet Security 2016
- AVIRA Antivirus Pro 15.0
- Bitdefender Internet Security 20.0
- BullGuard Internet Security 16.0
- Emsisoft Anti-Malware 11.0
- eScan Internet Security 14.0
- ESET Smart Security 9.0
- F-Secure Safe 14.150
- Fortinet FortiClient 5.2
- Kaspersky Internet Security 16.0
- Lavasoft Ad-Aware Pro Security 11.10
- McAfee Internet Security 18.0
- Microsoft Windows Defender 4.9
- Quick Heal Total Security 16.0
- Sophos Endpoint Security and Control 10.3
- Tencent PC Manager 11.2
- ThreatTrack Vipre Internet Security Pro 9.3
- 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 March 2016. Telemetry data was gathered for the files in the test over the period between January and March 2016. 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. If a family is in the low or very low partition and has less than 5 samples in the test set, then the family weight is multiplied by the number of samples in the test set divided by 5. 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 March 2016 for the File-Detection Test contained 163763 malware samples. The number of encounters caused by the malware samples used in the test was according to Microsoft's telemetry data around 2,931,597. The malware families represented by the test set had nearly 60 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.

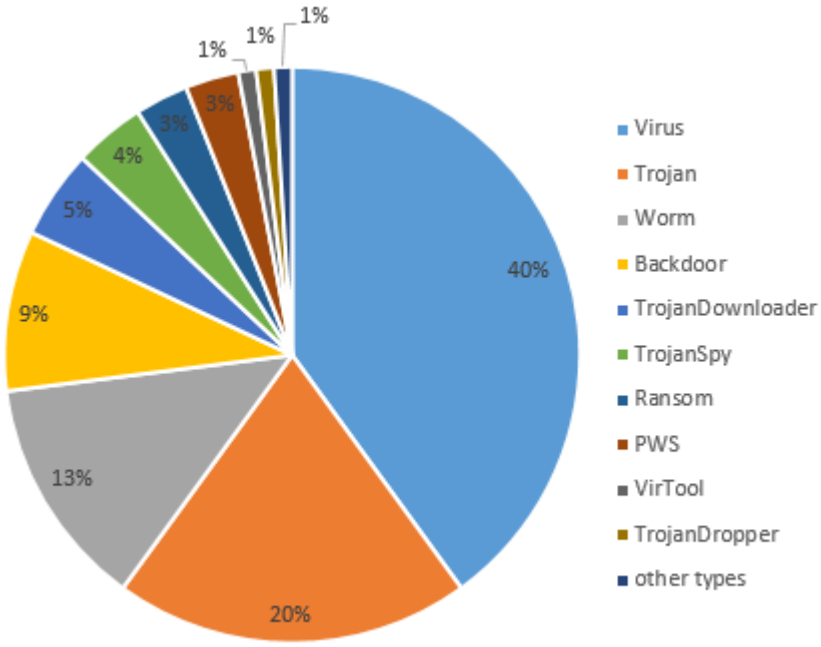
Top 15 most impacted countries:

1.	Myanmar	33.3%
2.	Pakistan	28.0%
3.	Indonesia	27.5%
4.	Mongolia	27.5%
5.	Palestina	26.2%
6.	Syria	24.7%
7.	Iran	24.4%
8.	Nepal	22.9%
9.	Tanzania	22.5%
10.	Bangladesh	21.5%
11.	Iraq	20.5%
12.	Algeria	20.3%
13.	Egypt	20.1%
14.	Vietnam	19.9%
15.	Ghana	19.7%

Top 15 less impacted countries:

1.	Japan	1.1%
2.	Finland	1.4%
3.	Norway	1.7%
4.	Denmark	1.8%
5.	Switzerland	1.8%
6.	United States	1.9%
7.	Sweden	2.0%
8.	Australia	2.1%
9.	New Zealand	2.1%
10.	United Kingdom	2.2%
11.	Ireland	2.2%
12.	Canada	2.2%
13.	Germany	2.3%
14.	Austria	2.4%
15.	Netherlands	2.5%

Distribution of Malware Types in the test-set



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

1. Virut	15.2% (High)	11. **Skeeyah**	2.4% (Very Low)
2. Ramnit	12.1% (High)	12. Upatre	2.2% (Low)
3. Sality	8.5% (High)	13. Dorkbot	1.5% (High)
4. Vobfus	5.0% (Moderate)	14. Ursnif	1.3% (Low)
5. Bladabindi	4.6% (High)	15. Mytonel	1.2% (High)
6. Kovter	3.4% (Moderate)	16. Tescrypt	1.2% (High)
7. Gamarue	3.3% (High)	17. Allaple	1.1% (Low)
8. Blakamba	3.0% (Moderate)	18. Parite	1.0% (Moderate)
9. **Dynamer**	2.5% (Very Low)	19. Chir	1.0% (Moderate)
10. Nivdort	2.5% (Moderate)	20. Lethic	1.0% (Low)

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

Malware Family	Ecosystem Computers
1. Gamarue	4594578
2. Peals	3747796
3. Dynamer	3586450
4. Skeeyah	3317590
5. Obfuscator	3168830
6. Spursint	2302993
7. Autorun	1997233
8. Jenxcus	1961297
9. Dorv	1406784
10. Ramnit	1317871

Top 10 Test Set Malware Families with highest Test Impact

Malware Family	Test Impact
1. Gamarue	24.0%
2. Ramnit	6.9%
3. Sality	5.6%
4. Phabeload	3.5%
5. Virut	3.1%
6. Bladabindi	2.6%
7. Jenxcus	2.5%
8. Tescrypt	2.2%
9. Nuqel	1.9%
10. Mytonel	1.9%

[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	99.9%	0.1%	*99.9%*	-
2. Kaspersky Lab	99.9%	0.1%	*99.9%*	-
3. Microsoft	99.7%	1.9%	*98.1%*	*+1.6%*
4. ESET	99.7%	0.6%	*99.4%*	*+0.3%*
5. F-Secure	99.7%	0.2%	*99.8%*	*-0.1%*
6. ThreatTrack	99.7%	0.2%	*99.8%*	*-0.1%*
7. Emsisoft	99.7%	0.2%	*99.8%*	*-0.1%*
8. Tencent	99.7%	0.2%	*99.8%*	*-0.1%*
9. Bitdefender	99.7%	0.2%	*99.8%*	*-0.1%*
10. BullGuard	99.7%	0.2%	*99.8%*	*-0.1%*
11. eScan	99.7%	0.2%	*99.8%*	*-0.1%*
12. Quick Heal	99.7%	0.2%	*99.8%*	*-0.1%*
13. Lavasoft	99.6%	0.3%	*99.7%*	*-0.1%*
14. Avast	99.6%	0.6%	*99.4%*	*+0.2%*
15. Fortinet	99.5%	0.6%	*99.4%*	*+0.1%*
16. McAfee	99.5%	1.1%	*98.9%*	*+0.6%*
17. AVG	99.1%	1.2%	*98.8%*	*+0.3%*
18. Trend Micro	99.0%	1.6%	*98.4%*	*+0.6%*
19. Sophos	98.0%	2.4%	*97.6%*	*+0.4%*

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 6 million reporting machines.

	Brazil	Canada	China	France	Germany	India	Italy	Japan	Mexico	Russia	South Korea	Spain	UK	USA
Avast	99,91%	99,99%	99,98%	99,98%	99,99%	99,92%	99,98%	100,0%	99,97%	99,99%	99,97%	99,98%	99,99%	99,99%
AVG	99,83%	99,98%	99,97%	99,96%	99,98%	99,86%	99,95%	99,99%	99,92%	99,93%	99,91%	99,96%	99,97%	99,98%
Avira	99,99%	100,0%	100,0%	100,0%	100,0%	99,99%	100,0%	100,0%	99,99%	99,99%	99,99%	99,99%	100,0%	100,0%
Bitdefender	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
BullGuard	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
Emsisoft	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
eScan	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
ESET	99,93%	99,99%	99,97%	99,98%	99,99%	99,93%	99,98%	99,99%	99,96%	99,96%	99,96%	99,98%	99,99%	99,99%
Fortinet	99,95%	99,99%	99,97%	99,99%	99,99%	99,93%	99,98%	100,0%	99,98%	99,89%	99,95%	99,98%	99,98%	99,99%
F-Secure	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
Kaspersky Lab	99,98%	100,0%	99,99%	100,0%	100,0%	99,98%	100,0%	100,0%	99,99%	100,0%	100,0%	100,0%	100,0%	100,0%
Lavasoft	99,94%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
McAfee	99,93%	99,97%	99,97%	99,98%	99,98%	99,91%	99,97%	99,99%	99,95%	99,94%	99,95%	99,97%	99,97%	99,95%
Microsoft	99,97%	99,99%	99,99%	99,99%	99,98%	99,96%	99,97%	100,0%	99,97%	99,98%	99,98%	99,96%	99,98%	99,99%
Quick Heal	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
Sophos	99,71%	99,94%	99,91%	99,93%	99,96%	99,44%	99,91%	99,98%	99,83%	99,87%	99,85%	99,92%	99,94%	99,94%
Tencent	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
ThreatTrack	99,95%	99,99%	99,99%	99,99%	99,98%	99,95%	99,97%	100,0%	99,97%	99,99%	99,99%	99,96%	99,98%	99,99%
Trend Micro	99,91%	99,98%	99,97%	99,97%	99,97%	99,82%	99,95%	99,99%	99,90%	99,85%	99,93%	99,96%	99,98%	99,98%

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. Bulgaria	5109 in 100000	11. Slovak Republic	950 in 100000
2. Ecuador	1730 in 100000	12. Czech Republic	912 in 100000
3. Macedonia	1358 in 100000	13. **Brazil**	906 in 100000
4. Honduras	1327 in 100000	14. **Turkey**	861 in 100000
5. Chile	1236 in 100000	15. Morocco	836 in 100000
6. Algeria	1233 in 100000	16. Portugal	831 in 100000
7. Peru	1166 in 100000	17. Israel	822 in 100000
8. Saudi Arabia	992 in 100000	18. Colombia	813 in 100000
9. Serbia	975 in 100000	19. Tunisia	777 in 100000
10. Venezuela	957 in 100000	20. Puerto Rico	728 in 100000

Global Non-Detection Risk: 430 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Binrop
3. Bladabindi
4. Ramnit
5. Nitol

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. Ecuador	4240 in 100000	11. Slovak Republic	1895 in 100000
2. Honduras	3329 in 100000	12. Puerto Rico	1771 in 100000
3. Chile	3050 in 100000	13. **Brazil**	1743 in 100000
4. Peru	2917 in 100000	14. Tunisia	1725 in 100000
5. Algeria	2865 in 100000	15. Iraq	1713 in 100000
6. Malaysia	2563 in 100000	16. **South Korea**	1678 in 100000
7. Venezuela	2456 in 100000	17. Colombia	1641 in 100000
8. Saudi Arabia	2285 in 100000	18. Israel	1610 in 100000
9. Czech Republic	2114 in 100000	19. Argentina	1530 in 100000
10. Morocco	1906 in 100000	20. Azerbaijan	1515 in 100000

Global Non-Detection Risk: 915 in 100000

Top 5 missed malware families:

1. Jenxcus
2. Bladabindi
3. Gamarue
4. Bunitu
5. Mytonel

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. Syria	340 in 100000	11. Estonia	259 in 100000
2. Azerbaijan	316 in 100000	12. Slovak Republic	257 in 100000
3. Latvia	314 in 100000	13. Kenya	256 in 100000
4. Moldova	313 in 100000	14. Croatia	253 in 100000
5. Georgia	298 in 100000	15. Austria	253 in 100000
6. Armenia	297 in 100000	16. Lithuania	242 in 100000
7. Albania	295 in 100000	17. Switzerland	238 in 100000
8. Bosnia and Herzegov.	288 in 100000	18. South Africa	229 in 100000
9. **Australia**	278 in 100000	19. Kazakhstan	228 in 100000
10. Kuwait	263 in 100000	20. Peru	225 in 100000

Global Non-Detection Risk: 32 in 100000

Top 5 missed malware families:
1. Lockscreen
2. Kegotip
3. Bancos
4. Gamarue
5. Ramnit

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. Austria	1348 in 100000	11. **Spain**	868 in 100000
2. Ecuador	1303 in 100000	12. Algeria	846 in 100000
3. Romania	1236 in 100000	13. Saudi Arabia	910 in 100000
4. Honduras	1077 in 100000	14. United Arab Emir.	824 in 100000
5. Chile	1030 in 100000	15. Greece	812 in 100000
6. Israel	948 in 100000	16. Switzerland	759 in 100000
7. Costa Rica	912 in 100000	17. **United Kingdom**	758 in 100000
8. Sweden	910 in 100000	18. Venezuela	738 in 100000
9. Peru	896 in 100000	19. Qatar	726 in 100000
10. **Germany**	871 in 100000	20. **Australia**	684 in 100000

Global Non-Detection Risk: 335 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Tofsee
4. Chicrypt
5. Bladabindi

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):

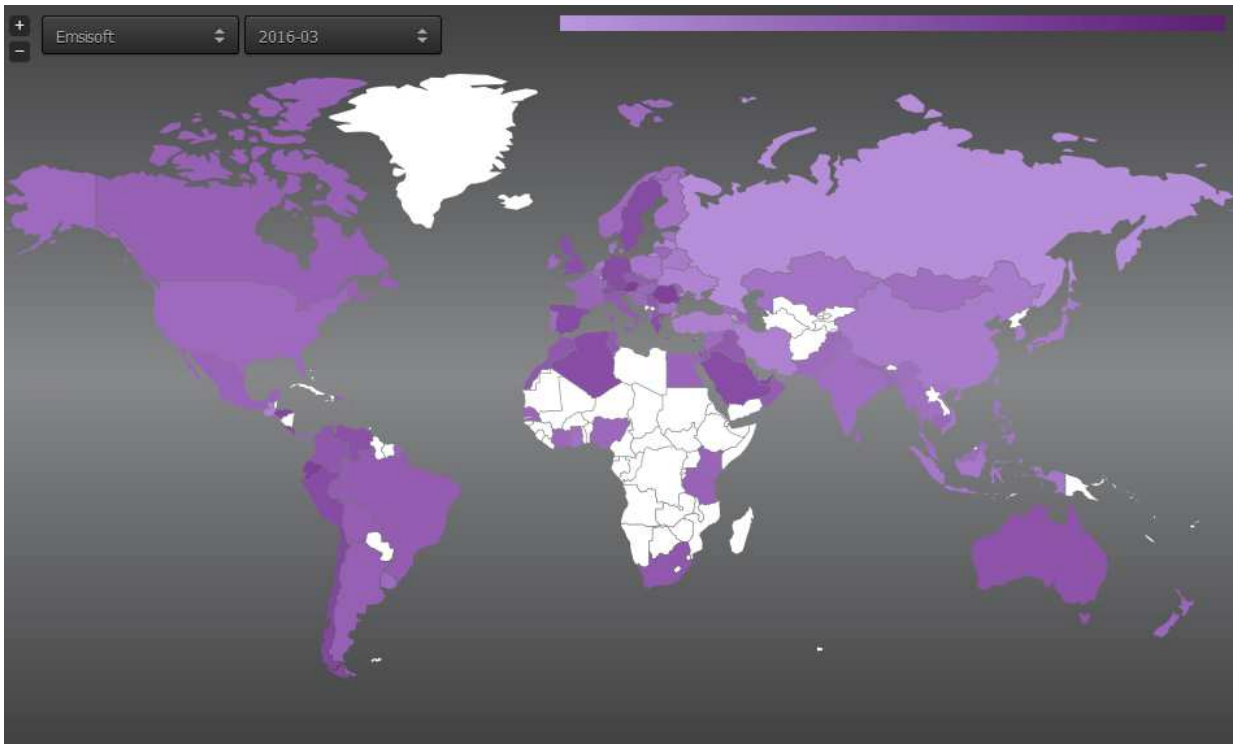
1. Austria	1348 in 100000	11. **Spain**	868 in 100000
2. Ecuador	1303 in 100000	12. Algeria	846 in 100000
3. Romania	1236 in 100000	13. Saudi Arabia	833 in 100000
4. Honduras	1077 in 100000	14. United Arab Emir.	824 in 100000
5. Chile	1030 in 100000	15. Greece	812 in 100000
6. Israel	948 in 100000	16. Switzerland	759 in 100000
7. Costa Rica	912 in 100000	17. **United Kingdom**	758 in 100000
8. Sweden	910 in 100000	18. Venezuela	738 in 100000
9. Peru	896 in 100000	19. Qatar	726 in 100000
10. **Germany**	871 in 100000	20. **Australia**	684 in 100000

Global Non-Detection Risk: 335 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Tofsee
4. Chicrypt
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. Austria	1345 in 100000	11. **Spain**	866 in 100000
2. Ecuador	1301 in 100000	12. Algeria	844 in 100000
3. Romania	1234 in 100000	13. Saudi Arabia	831 in 100000
4. Honduras	1075 in 100000	14. United Arab Emir.	823 in 100000
5. Chile	1027 in 100000	15. Greece	810 in 100000
6. Israel	946 in 100000	16. Switzerland	757 in 100000
7. Costa Rica	910 in 100000	17. **United Kingdom**	756 in 100000
8. Sweden	907 in 100000	18. Venezuela	736 in 100000
9. Peru	894 in 100000	19. Qatar	723 in 100000
10. **Germany**	868 in 100000	20. **Australia**	682 in 100000

Global Non-Detection Risk: 333 in 100000

Top 5 missed malware families:

1. Jenxcus
2. Nivdort
3. Tofsee
4. Chicrypt
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. Austria	1348 in 100000	11. **Spain**	868 in 100000
2. Ecuador	1303 in 100000	12. Algeria	846 in 100000
3. Romania	1236 in 100000	13. Saudi Arabia	833 in 100000
4. Honduras	1077 in 100000	14. United Arab Emir.	824 in 100000
5. Chile	1030 in 100000	15. Greece	812 in 100000
6. Israel	948 in 100000	16. Switzerland	759 in 100000
7. Costa Rica	912 in 100000	17. **United Kingdom**	758 in 100000
8. Sweden	910 in 100000	18. Venezuela	738 in 100000
9. Peru	896 in 100000	19. Qatar	726 in 100000
10. **Germany**	871 in 100000	20. **Australia**	684 in 100000

Global Non-Detection Risk: 335 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Tofsee
4. Chicrypt
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. Honduras	1520 in 100000	11. El Salvador	1022 in 100000
2. Azerbaijan	1135 in 100000	12. Algeria	1022 in 100000
3. Ecuador	1122 in 100000	13. Puerto Rico	1020 in 100000
4. Chile	1111 in 100000	14. Albania	1011 in 100000
5. Peru	1093 in 100000	15. Uruguay	1009 in 100000
6. Syria	1061 in 100000	16. Senegal	1000 in 100000
7. Kuwait	1041 in 100000	17. Armenia	998 in 100000
8. Jamaica	1040 in 100000	18. Panama	996 in 100000
9. Moldova	1035 in 100000	19. Georgia	995 in 100000
10. Slovak Republic	1034 in 100000	20. Bosnia and Herzeg.	962 in 100000

Global Non-Detection Risk: 304 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Brobanlaw
3. Lockscreen
4. Adload
5. Lurka

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):

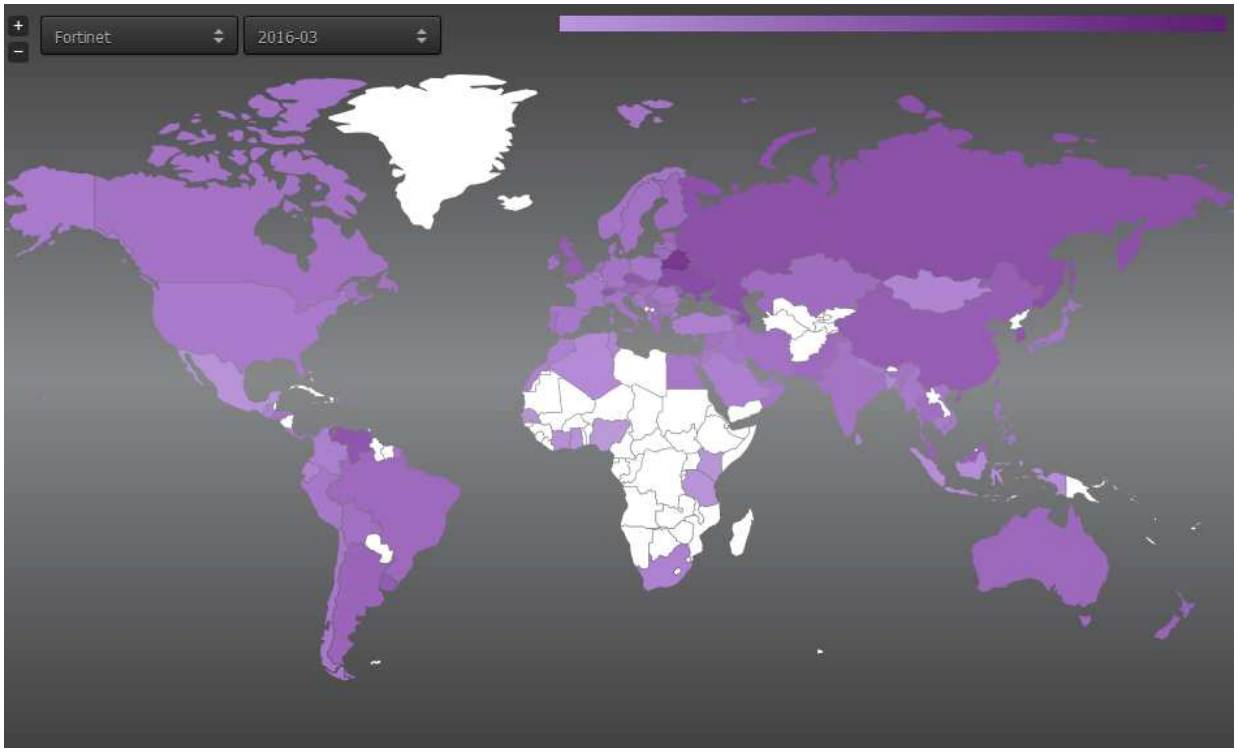
1. Ecuador	1301 in 100000	11. Algeria	840 in 100000
2. Romania	1228 in 100000	12. Saudi Arabia	820 in 100000
3. Austria	1174 in 100000	13. **Germany**	813 in 100000
4. Honduras	1076 in 100000	14. United Arab Emir.	807 in 100000
5. Chile	1026 in 100000	15. Greece	802 in 100000
6. Israel	940 in 100000	16. **United Kingdom**	743 in 100000
7. Costa Rica	909 in 100000	17. Venezuela	736 in 100000
8. Sweden	903 in 100000	18. Switzerland	730 in 100000
9. Peru	893 in 100000	19. Qatar	715 in 100000
10. **Spain**	860 in 100000	20. **Australia**	673 in 100000

Global Non-Detection Risk: 312 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Tofsee
4. Bladabindi
5. Gamarue

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. Belarus	2155 in 100000	11. **United Kingdom**	732 in 100000
2. Ukraine	1169 in 100000	12. Slovak Republic	730 in 100000
3. Azerbaijan	1149 in 100000	13. Singapore	723 in 100000
4. **Russian Federation**	1073 in 100000	14. Moldova	689 in 100000
5. **South Korea**	935 in 100000	15. Malaysia	661 in 100000
6. Venezuela	929 in 100000	16. New Zealand	659 in 100000
7. Czech Republic	913 in 100000	17. Armenia	636 in 100000
8. Switzerland	885 in 100000	18. Slovenia	616 in 100000
9. Uruguay	788 in 100000	19. Argentina	608 in 100000
10. **China**	735 in 100000	20. Taiwan	594 in 100000

Global Non-Detection Risk: 503 in 100000

Top 5 missed malware families:
1. Induc
2. Nuqel
3. Bladabindi
4. Caphaw
5. Nitol

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. Ecuador	605 in 100000	11. Colombia	220 in 100000
2. Honduras	508 in 100000	12. Azerbaijan	216 in 100000
3. Peru	416 in 100000	13. Nepal	212 in 100000
4. Chile	398 in 100000	14. Jamaica	204 in 100000
5. Algeria	393 in 100000	15. Panama	199 in 100000
6. Venezuela	333 in 100000	16. Iraq	199 in 100000
7. Saudi Arabia	296 in 100000	17. Kuwait	190 in 100000
8. Morocco	250 in 100000	18. Oman	189 in 100000
9. Puerto Rico	244 in 100000	19. **Brazil**	188 in 100000
10. Tunisia	234 in 100000	20. Jordan	187 in 100000

Global Non-Detection Risk: 89 in 100000

Top 5 missed malware families:

1. Jenxcus
2. Ursnif
3. Coolvidoor
4. Chkbot
5. Evotob

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):

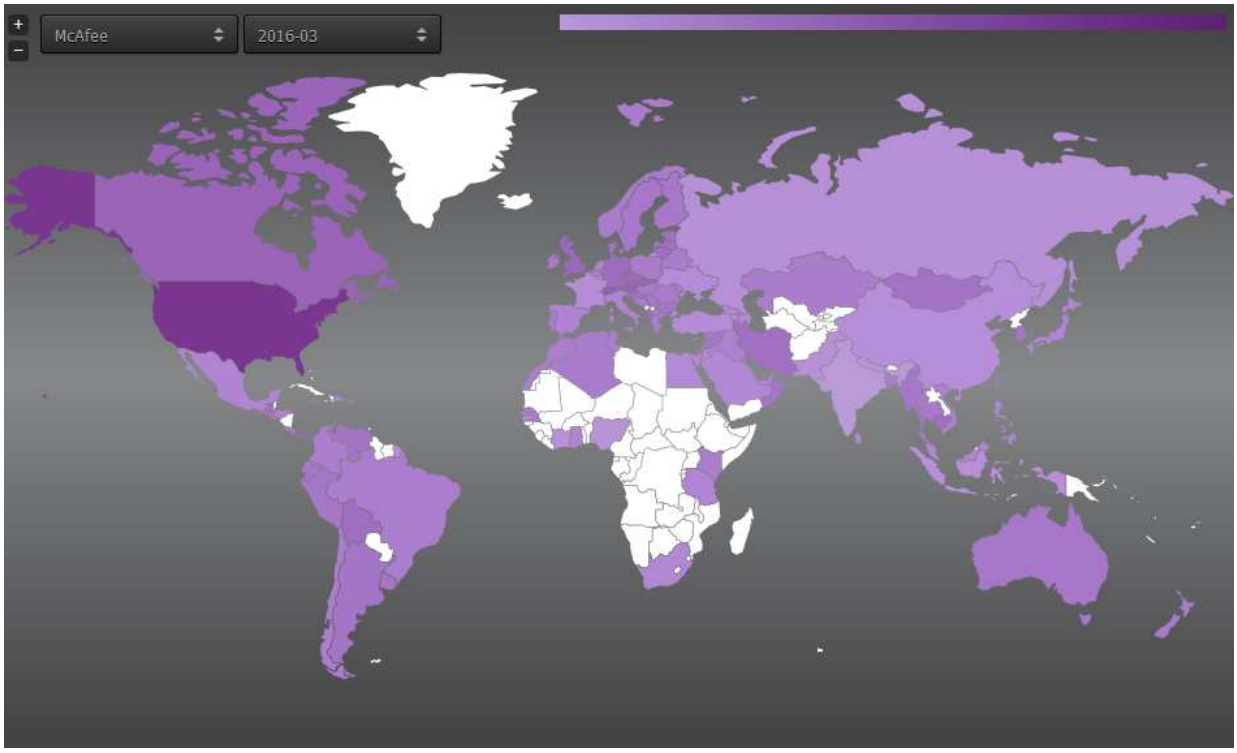
1. Austria	1405 in 100000	11. Algeria	904 in 100000
2. Ecuador	1354 in 100000	12. **Spain**	900 in 100000
3. Romania	1278 in 100000	13. Saudi Arabia	892 in 100000
4. Honduras	1163 in 100000	14. United Arab Emir.	873 in 100000
5. Chile	1078 in 100000	15. Greece	871 in 100000
6. Israel	1013 in 100000	16. Switzerland	818 in 100000
7. Costa Rica	988 in 100000	17. Czech Republic	811 in 100000
8. Sweden	968 in 100000	18. Qatar	798 in 100000
9. Peru	941 in 100000	19. **United Kingdom**	797 in 100000
10. **Germany**	908 in 100000	20. Venezuela	784 in 100000

Global Non-Detection Risk: 363 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Bladabindi
4. Tofsee
5. Chicrypt

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. **United States**	2862 in 100000	11. Lithuania	1010 in 100000
2. Switzerland	1383 in 100000	12. Bolivia	1009 in 100000
3. Austria	1241 in 100000	13. Guatemala	1005 in 100000
4. **Canada**	1224 in 100000	14. Albania	1003 in 100000
5. United Kingdom	1153 in 100000	15. Iran	996 in 100000
6. Slovak Republic	1148 in 100000	16. Latvia	994 in 100000
7. Panama	1120 in 100000	17. Slovenia	970 in 100000
8. Czech Republic	1105 in 100000	18. Estonia	962 in 100000
9. **Germany**	1057 in 100000	19. Denmark	935 in 100000
10. Cambodia	1015 in 100000	20. Mongolia	932 in 100000

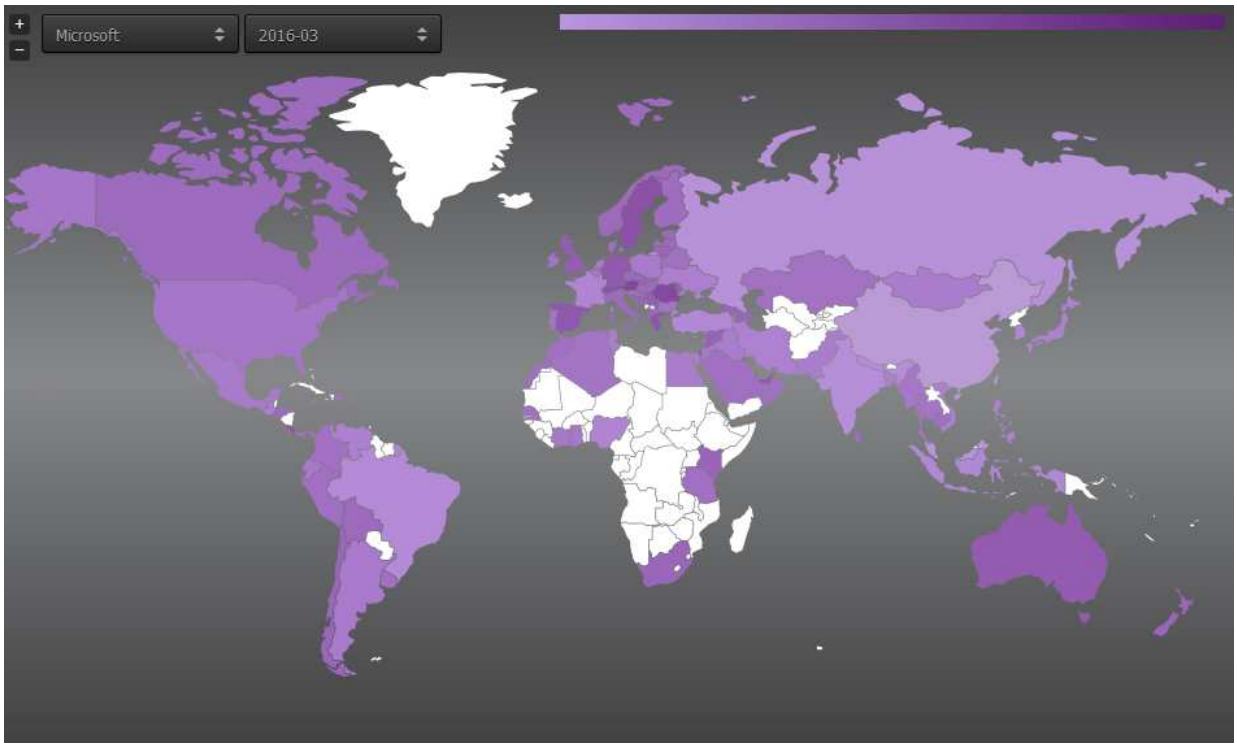
Global Non-Detection Risk: 525 in 100000

Top 5 missed malware families:

1. Gamarue
2. Bladabindi
3. Kovter
4. Nitol
5. Reffus

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. Austria	1565 in 100000	11. **Australia**	1011 in 100000
2. Romania	1486 in 100000	12. Cyprus	993 in 100000
3. Sweden	1451 in 100000	13. **United Kingdom**	986 in 100000
4. Costa Rica	1232 in 100000	14. Moldova	986 in 100000
5. Switzerland	1202 in 100000	15. Serbia	962 in 100000
6. Greece	1165 in 100000	16. Qatar	961 in 100000
7. **Spain**	1122 in 100000	17. Kuwait	940 in 100000
8. **Germany**	1100 in 100000	18. Syria	938 in 100000
9. United Arab Emir.	1063 in 100000	19. Bosnia and Herzeg.	921 in 100000
10. Israel	1011 in 100000	20. Slovak Republic	898 in 100000

Global Non-Detection Risk: 279 in 100000

Top 5 missed malware families:

1. Nivdort
2. Gamarue
3. Lockscreen
4. Tofsee
5. Survins

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. Austria	1353 in 100000	11. **Spain**	871 in 100000
2. Ecuador	1305 in 100000	12. Algeria	852 in 100000
3. Romania	1240 in 100000	13. Saudi Arabia	842 in 100000
4. Honduras	1078 in 100000	14. United Arab Emir.	829 in 100000
5. Chile	1033 in 100000	15. Greece	819 in 100000
6. Israel	958 in 100000	16. **United Kingdom**	764 in 100000
7. Sweden	918 in 100000	17. Switzerland	764 in 100000
8. Costa Rica	915 in 100000	18. Venezuela	740 in 100000
9. Peru	897 in 100000	19. Qatar	731 in 100000
10. **Germany**	877 in 100000	20. **Australia**	688 in 100000

Global Non-Detection Risk: 340 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Bladabindi
4. Tofsee
5. Chicrypt

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. Honduras	5229 in 100000	11. Panama	3335 in 100000
2. Ecuador	5162 in 100000	12. **United States**	3272 in 100000
3. Algeria	4674 in 100000	13. **India**	3195 in 100000
4. Cote d'Ivoire	4261 in 100000	14. Saudi Arabia	3192 in 100000
5. Senegal	4153 in 100000	15. El Salvador	3125 in 100000
6. Peru	4051 in 100000	16. Hong Kong	3070 in 100000
7. Georgia	4048 in 100000	17. Slovak Republic	3036 in 100000
8. Chile	3827 in 100000	18. Czech Republic	3032 in 100000
9. Venezuela	3638 in 100000	19. Tunisia	3028 in 100000
10. Ghana	3465 in 100000	20. Puerto Rico	3011 in 100000

Global Non-Detection Risk: 1971 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Gamarue
3. Psyokym
4. Kovter
5. Macoute

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. Austria	1347 in 100000	11. **Spain**	867 in 100000
2. Ecuador	1303 in 100000	12. Algeria	844 in 100000
3. Romania	1235 in 100000	13. Saudi Arabia	832 in 100000
4. Honduras	1077 in 100000	14. United Arab Emir.	823 in 100000
5. Chile	1029 in 100000	15. Greece	811 in 100000
6. Israel	946 in 100000	16. Switzerland	758 in 100000
7. Costa Rica	912 in 100000	17. **United Kingdom**	757 in 100000
8. Sweden	908 in 100000	18. Venezuela	738 in 100000
9. Peru	895 in 100000	19. Qatar	725 in 100000
10. **Germany**	870 in 100000	20. **Australia**	683 in 100000

Global Non-Detection Risk: 335 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Tofsee
4. Chicrypt
5. Bladabindi

ThreatTrack

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):

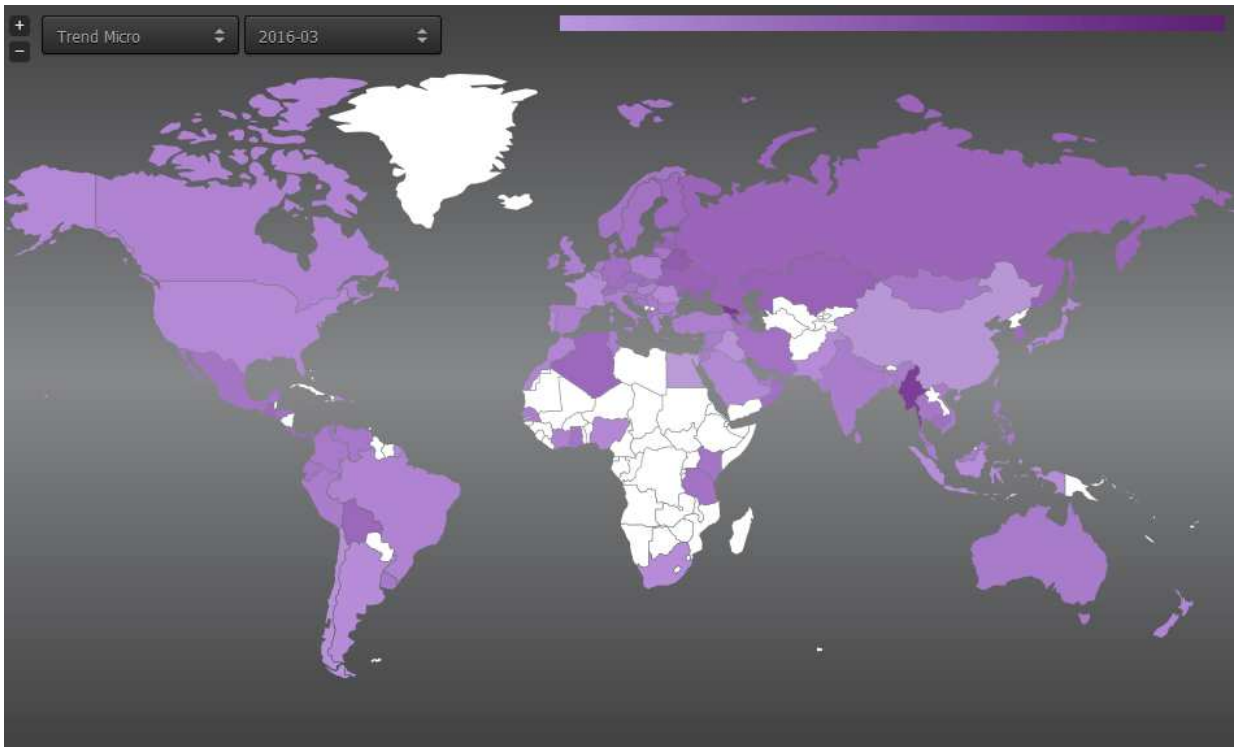
1. Ecuador	1338 in 100000	11. Algeria	867 in 100000
2. Romania	1250 in 100000	12. Saudi Arabia	838 in 100000
3. Austria	1204 in 100000	13. United Arab Emir.	829 in 100000
4. Honduras	1144 in 100000	14. Greece	828 in 100000
5. Chile	1067 in 100000	15. **Germany**	819 in 100000
6. Costa Rica	966 in 100000	16. Venezuela	769 in 100000
7. Israel	965 in 100000	17. Switzerland	762 in 100000
8. Sweden	928 in 100000	18. **United Kingdom**	754 in 100000
9. Peru	924 in 100000	19. Qatar	753 in 100000
10. **Spain**	877 in 100000	20. Cyprus	698 in 100000

Global Non-Detection Risk: 316 in 100000

Top 5 missed malware families:
1. Jenxcus
2. Nivdort
3. Tofsee
4. Gamarue
5. Bladabindi

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. Georgia	3037 in 100000	11. Algeria	1427 in 100000
2. Myanmar	2810 in 100000	12. Estonia	1403 in 100000
3. Armenia	2279 in 100000	13. Finland	1390 in 100000
4. Belarus	1763 in 100000	14. Guatemala	1376 in 100000
5. Latvia	1575 in 100000	15. Panama	1374 in 100000
6. Kazakhstan	1574 in 100000	16. **South Korea**	1330 in 100000
7. Ukraine	1556 in 100000	17. El Salvador	1318 in 100000
8. **Russian Federation**	1481 in 100000	18. Czech Republic	1303 in 100000
9. Moldova	1435 in 100000	19. Slovak Republic	1276 in 100000
10. Bolivia	1433 in 100000	20. **Germany**	1273 in 100000

Global Non-Detection Risk: 997 in 100000

Top 5 missed malware families:
1. Gamarue
2. Mytonel
3. Conustr
4. Bladabindi
5. Genmaldow

Copyright and Disclaimer

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

AV-Comparatives (April 2016)