AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Useful and useless statistics about viruses and anti-virus programs

Dipl.-Ing. Maik Morgenstern and Hendrik Pilz
AV-Test GmbH, Magdeburg, Germany

Presented at CARO 2010 Helsinki

http://www.av-test.org

Agenda

- Disclaimer
- The Average Anti-Malware Product
- The Average Malware
- A Typical Day in Anti-Malware Industry
- (Serious and not so Serious) Implications
- Conclusions
- Q&A

Disclaimer

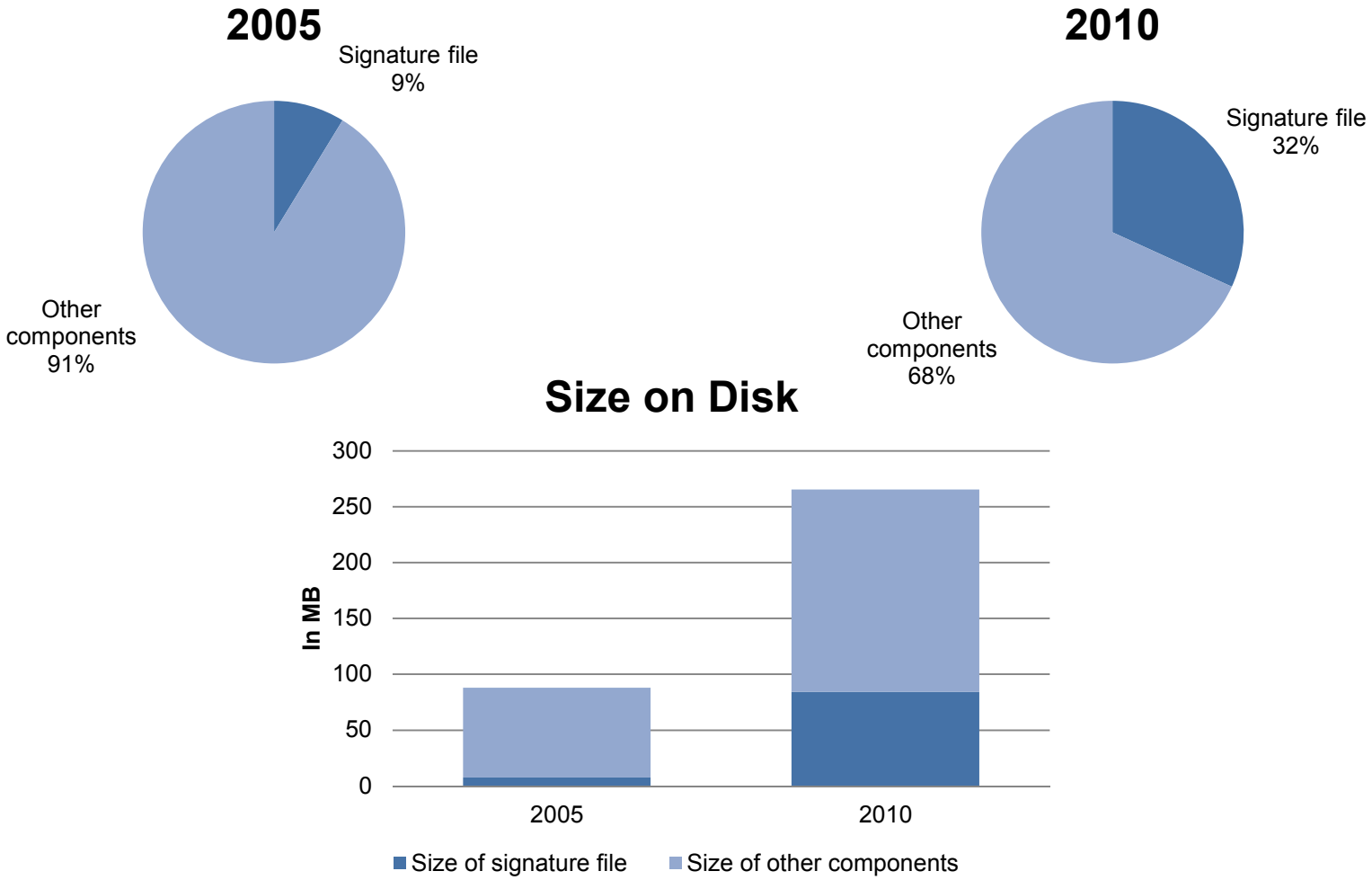
- Not necessarily a scientific presentation
- Bases on data from AV-Test only
- May not be representative
- We are just talking about numbers
- We are not claiming anything and we could be wrong with what we say
- Still, some numbers may be interesting

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The Average Anti-Malware Product

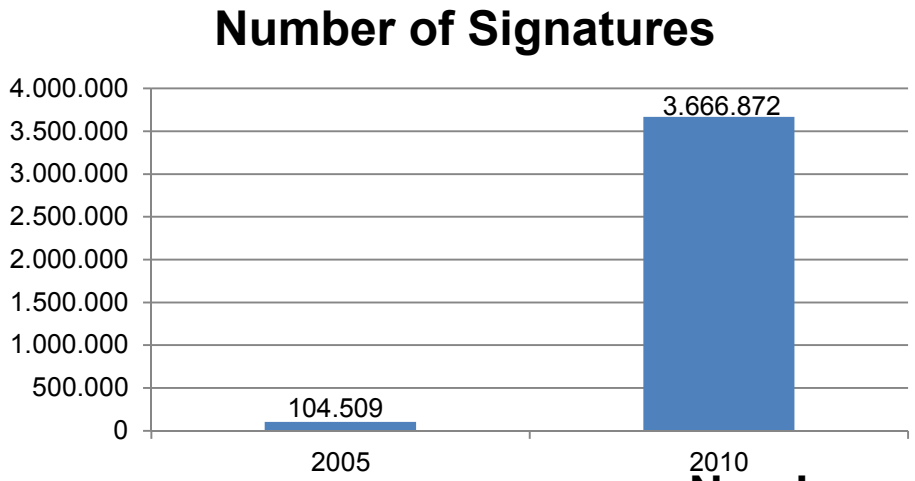
	2005	2010
Installer Size	12,6 MB	69,6 MB
Size on Disk	87,9 MB	265,5 MB
Number of Signatures	104.509	3.666.872
Size of Signature File	7,7 MB	84,4 MB
Price	45 €	32 €
Updates per Day	2	6
WildList Detection	(virtually) 100%	(virtually) 100%
Zoo Detection	93,04%	91,59%
False Positives	0,03%	0,00157%

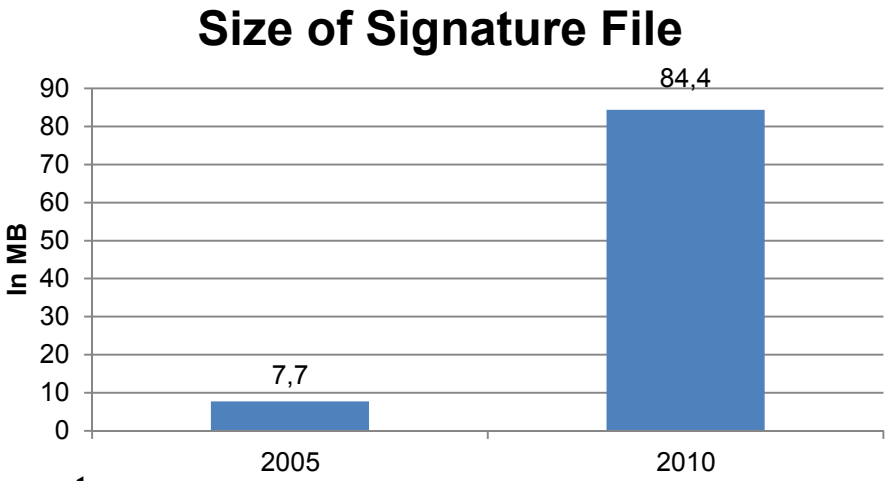
The Average Anti-Malware Product

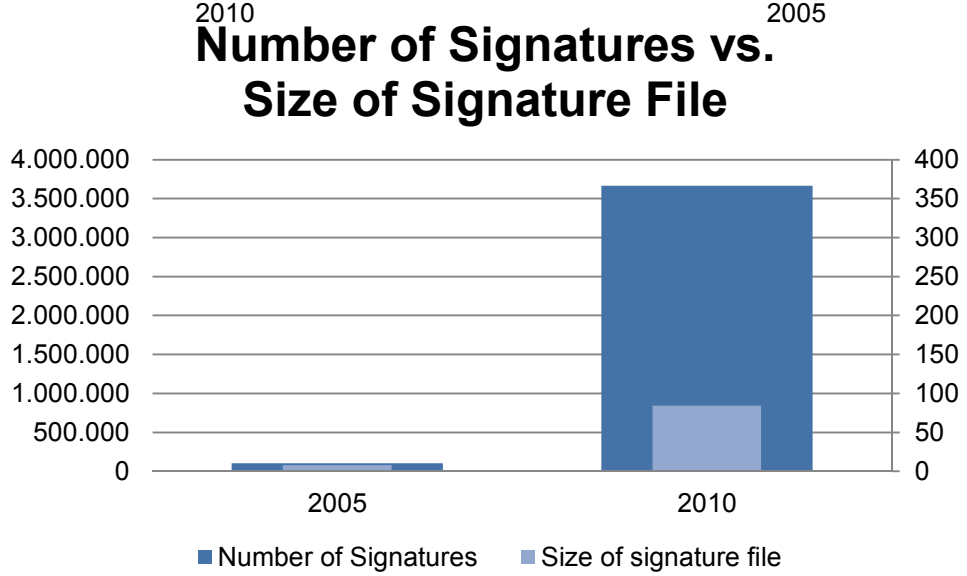


AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The Average Anti-Malware Product

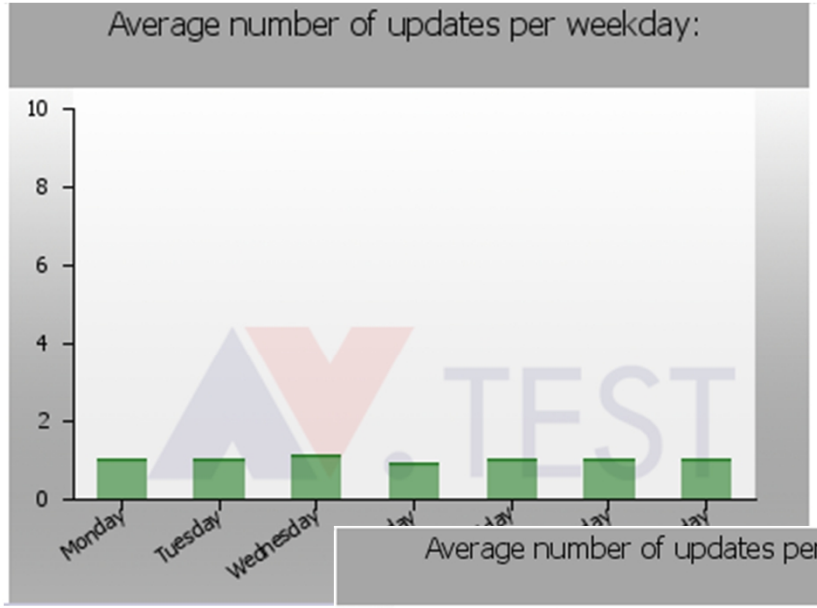


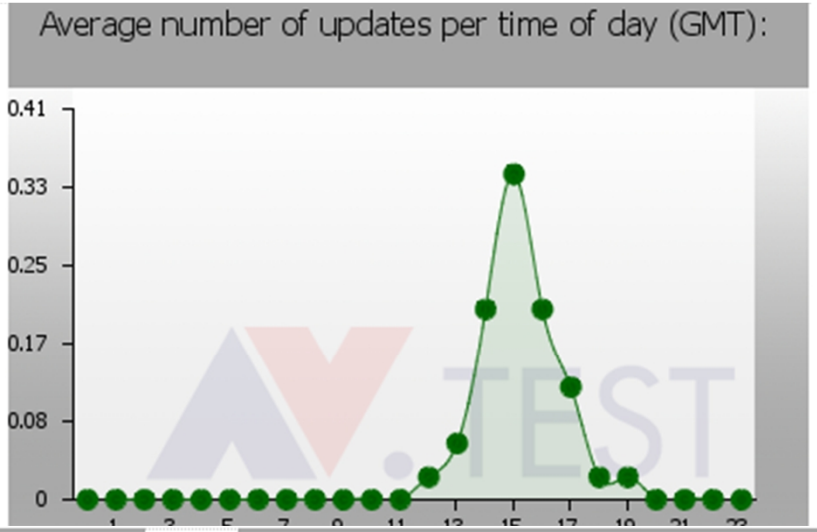




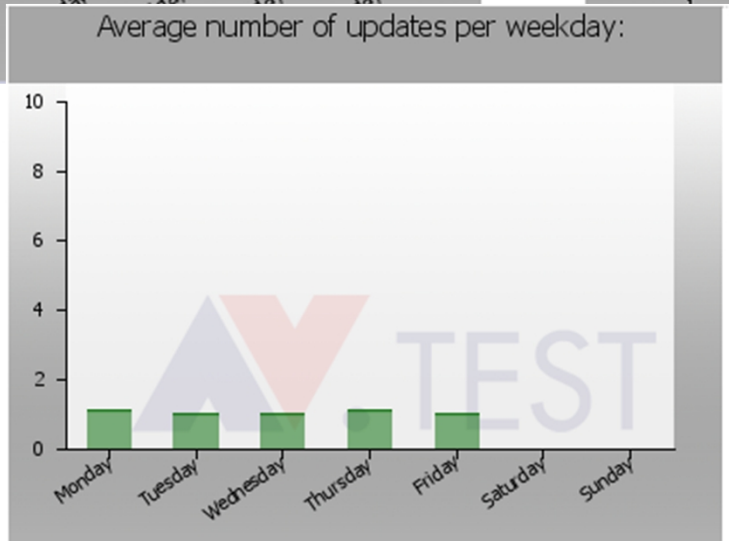
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

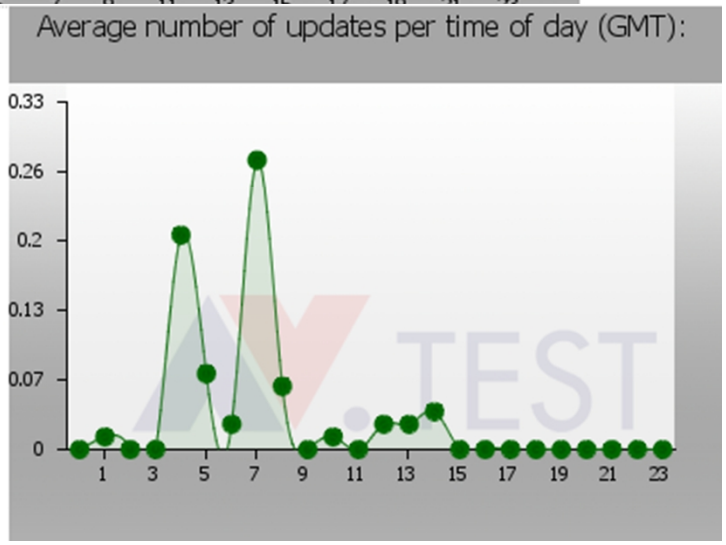
The Average Anti-Malware Product





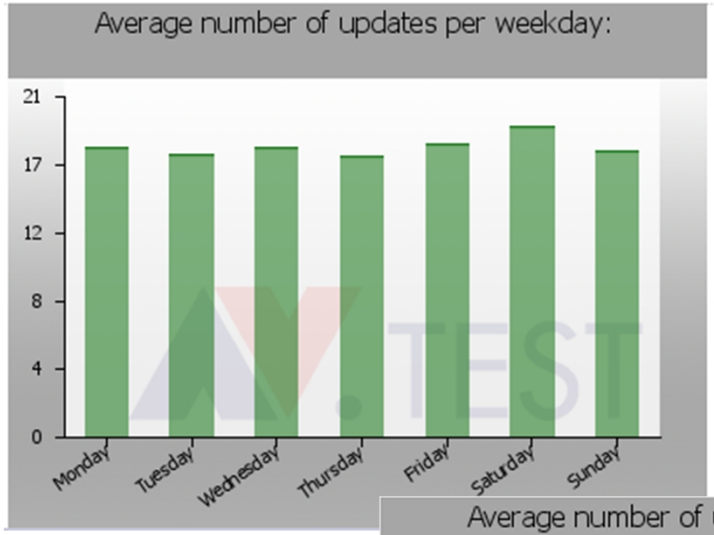
2005

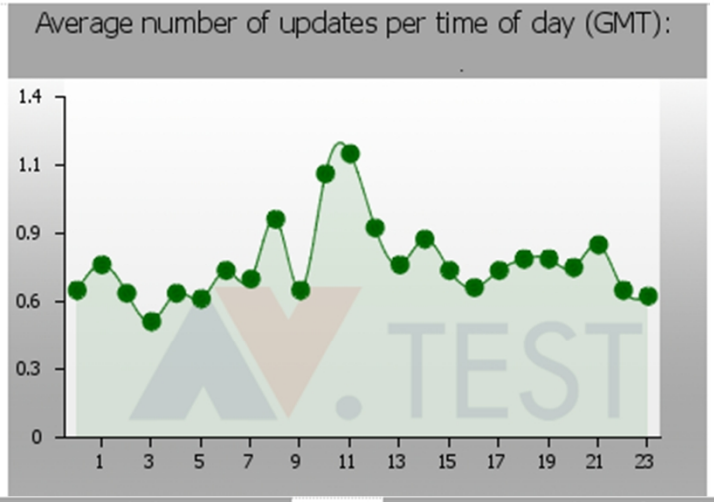




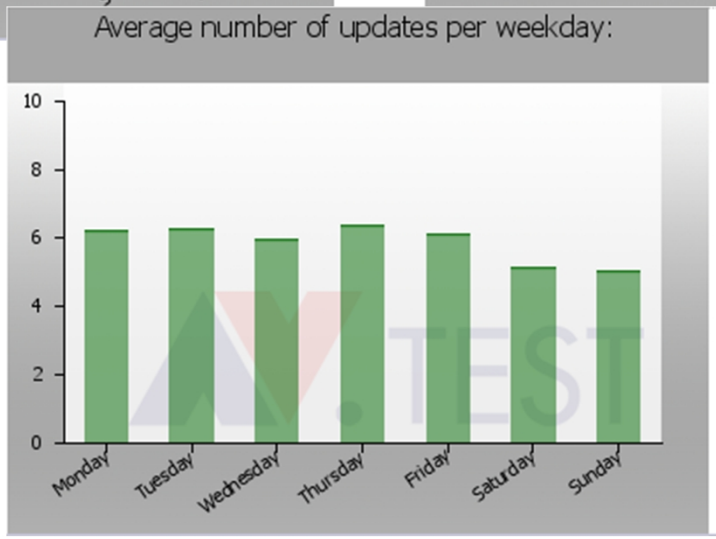
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

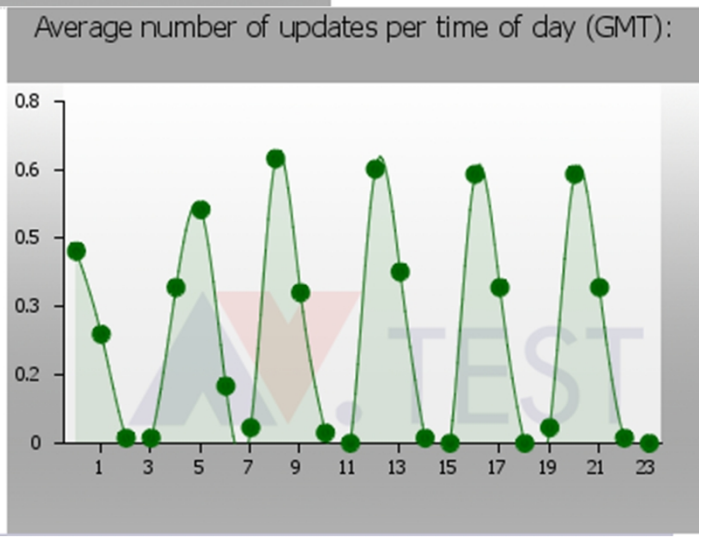
The Average Anti-Malware Product





2010

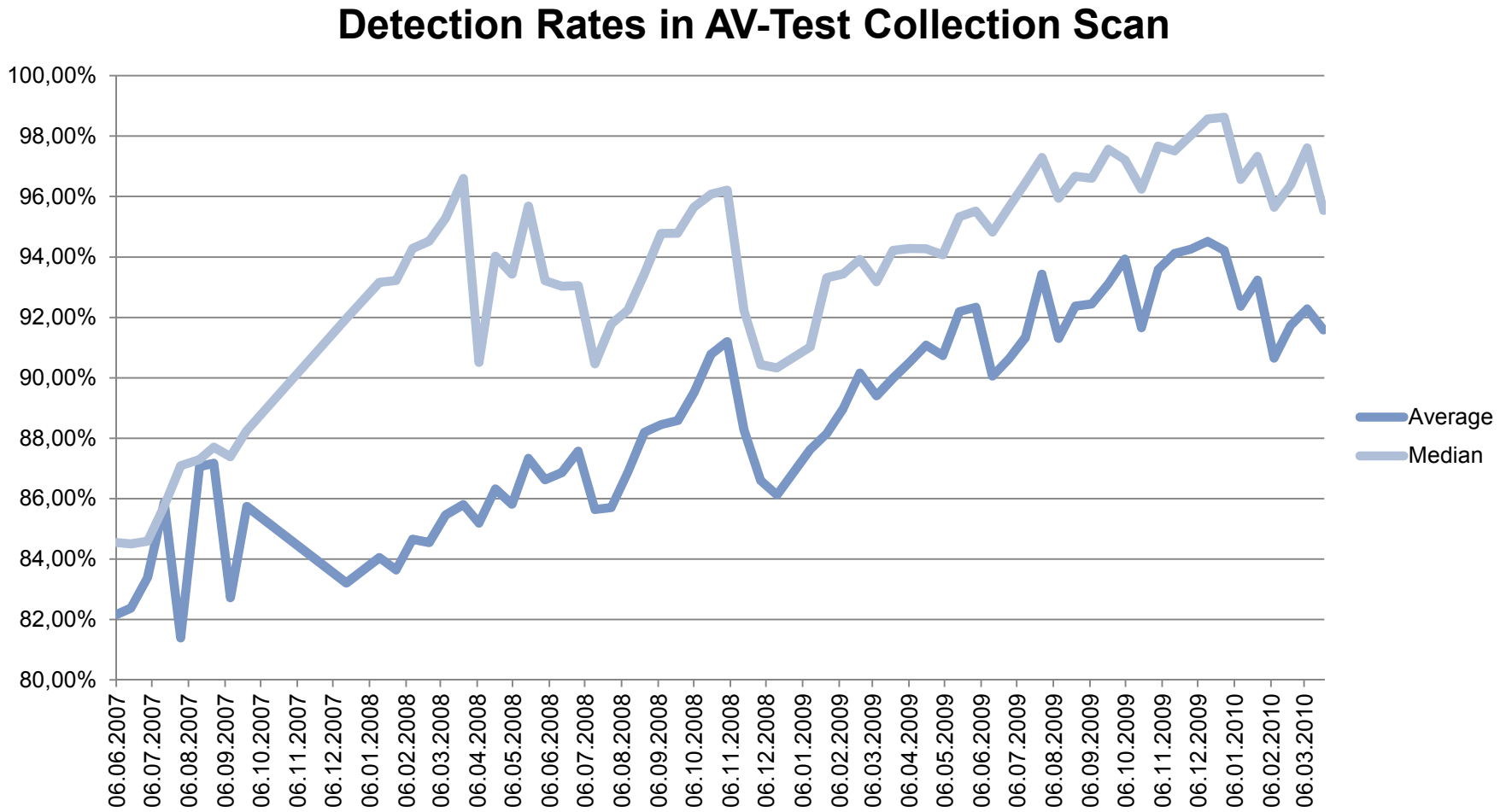




Up-To-Date Information:
http://www.av-test.org/numbers.php

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The Average Anti-Malware Product



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The Average Malware

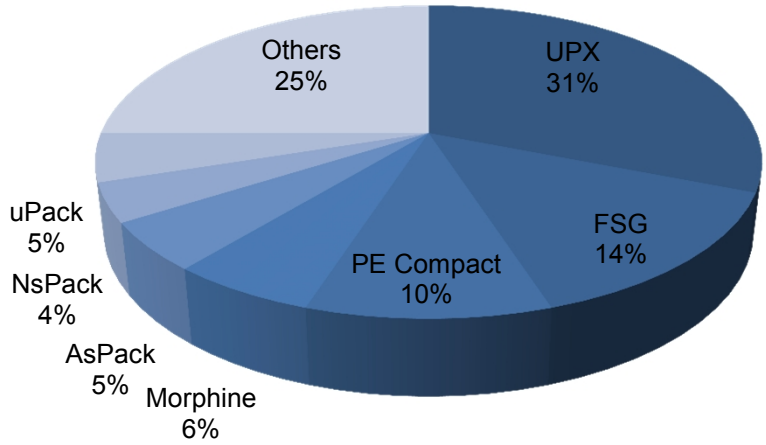
	2005	2010
Size	180 KB	486 KB
File Type	PE	PE
Malware Type	Trojan	Trojan
Packed by …	UPX	Custom Packer
Detected after …	10-12 hours	2-4 hours
Detected as …	Same Family	Several Different Names

The Average Malware

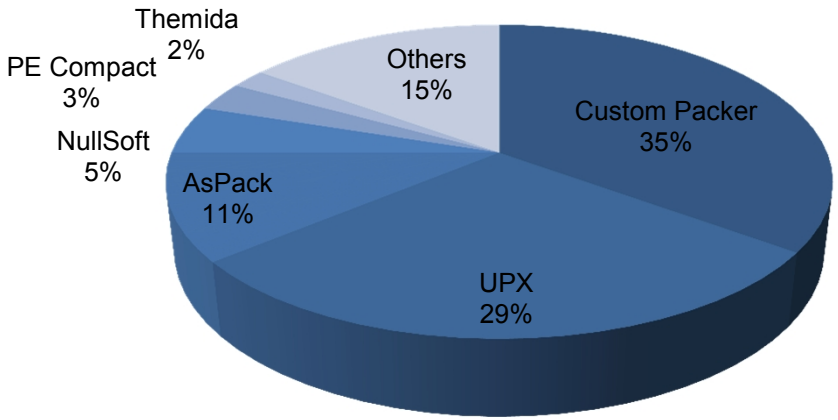
File Types	2005	2010
1.	PE Files	PE Files
2.	HTML/PHP/JavaScript	HTML/PHP/JavaScript
3.	Batch File/Scripts	PDF/Flash/Images

The Average Malware

Packers used in 2005

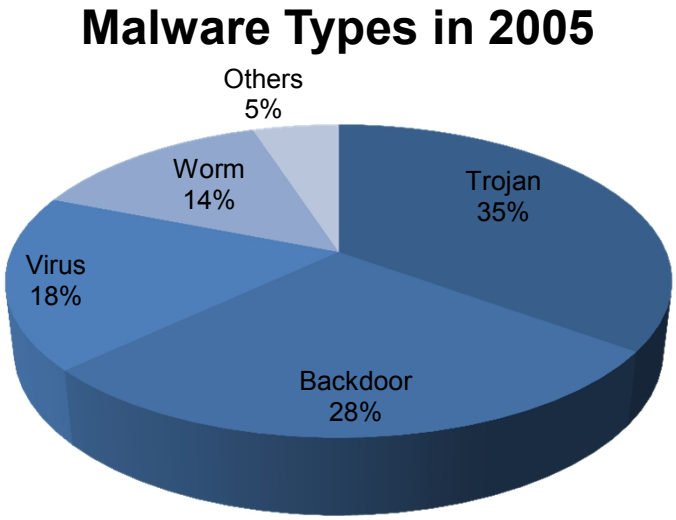


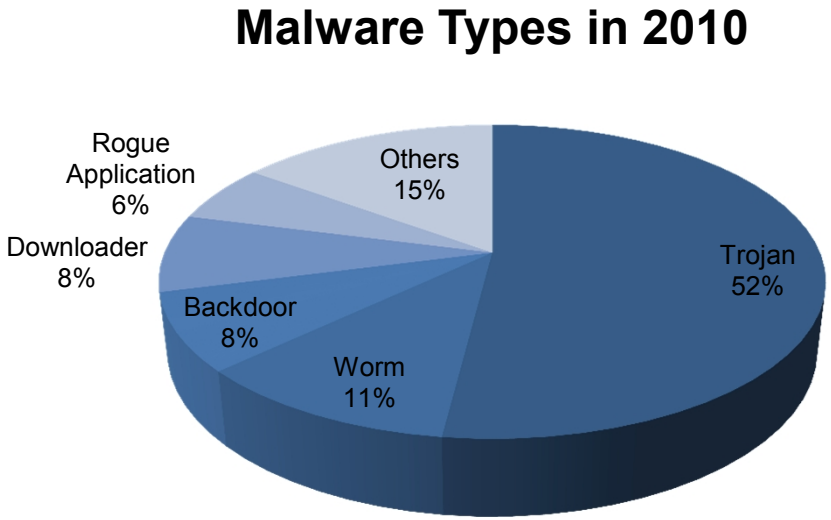
Packers used in 2010



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

The Average Malware





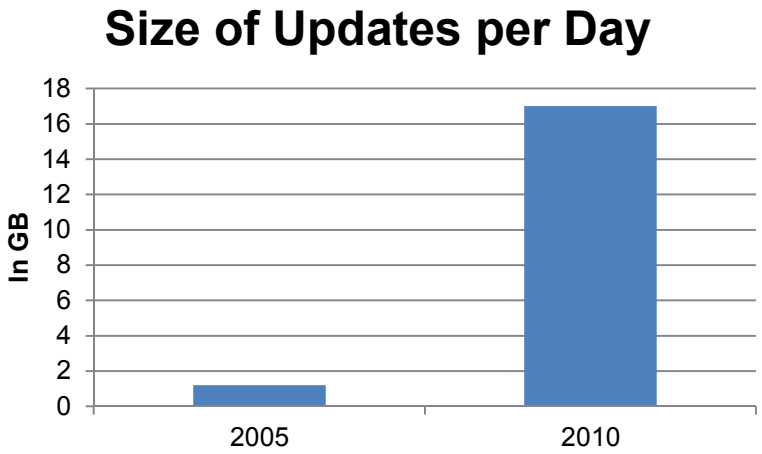
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

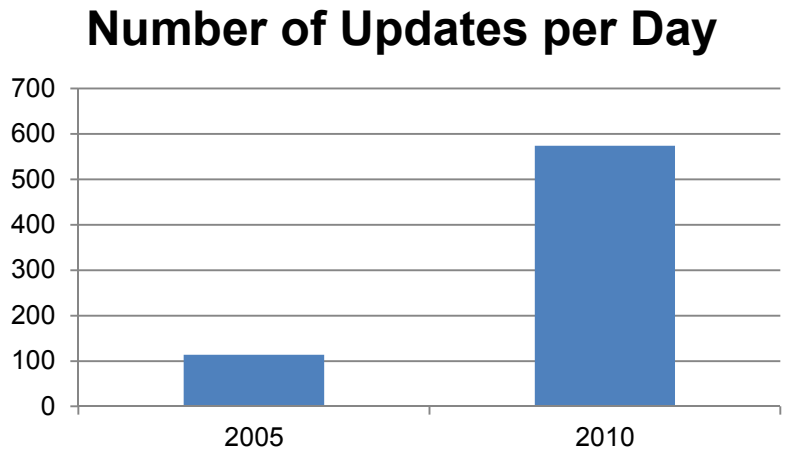
A Typical Day in Anti-Malware Industry

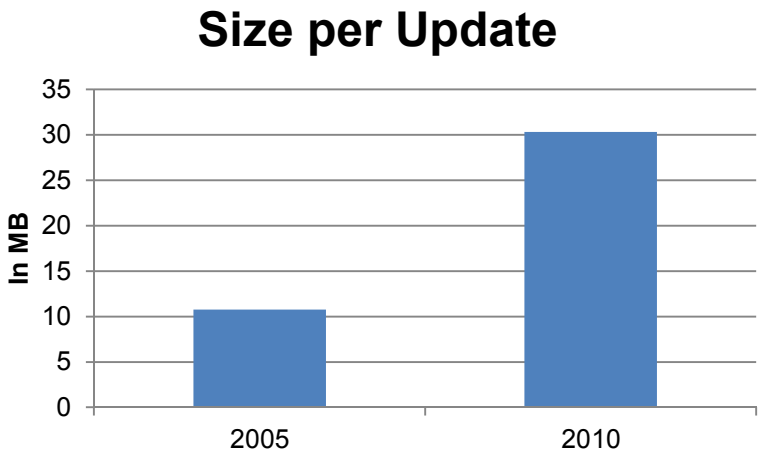
	2005	2010
Signature/Program Updates		
per Day	110	574
per Month	Over 3.400	Over 17.000
per Year	Over 40.000	Over 200.000
Size of the Updates		
per Day	1,2 GB	17 GB
per Month	Over 30 GB	Over 500 GB
per Year	Over 400 GB	Over 6.120 GB
New Malware		
per Day	360	Over 50.000
per Month	Over 10.000	Over 1.500.000
per Year	Nearly 130.000	Nearly 20.000.000

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

A Typical Day in Anti-Malware Industry

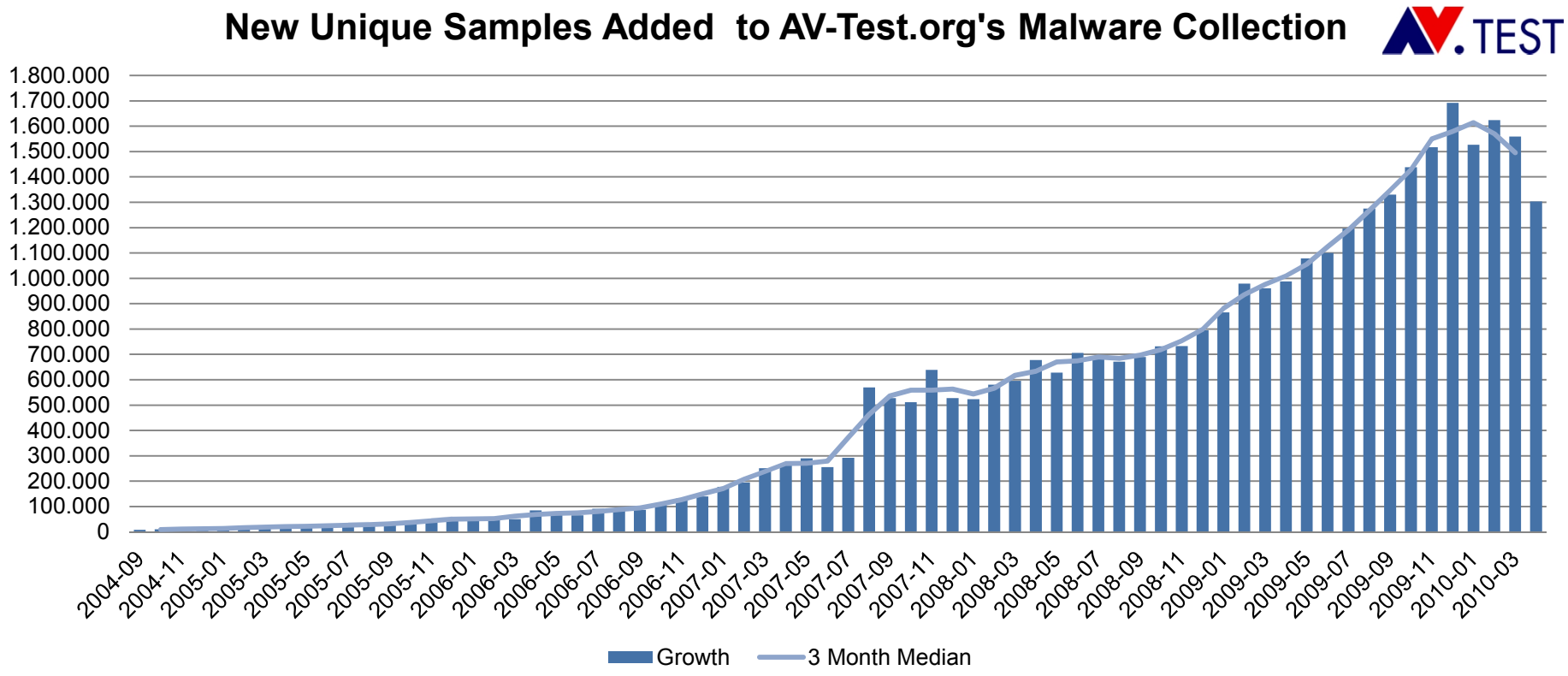






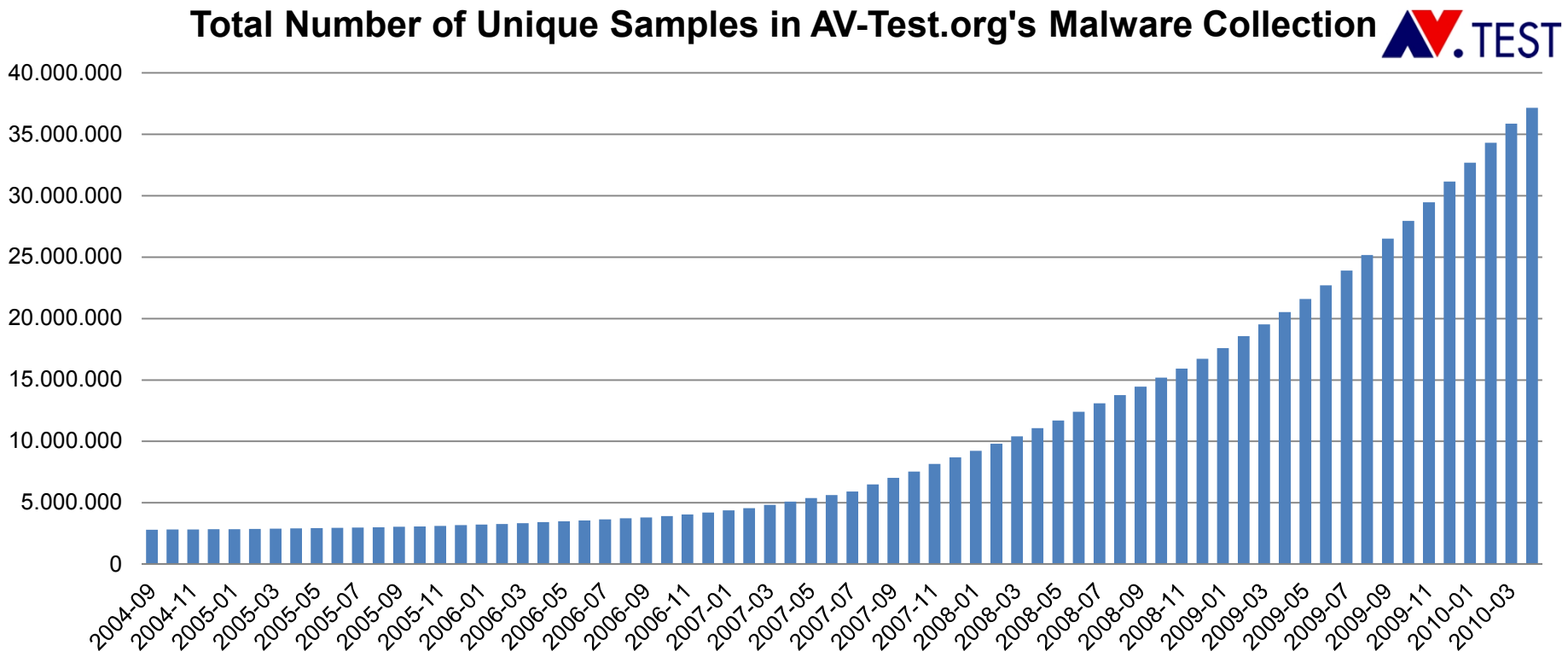
AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

A Typical Day in Anti-Malware Industry



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

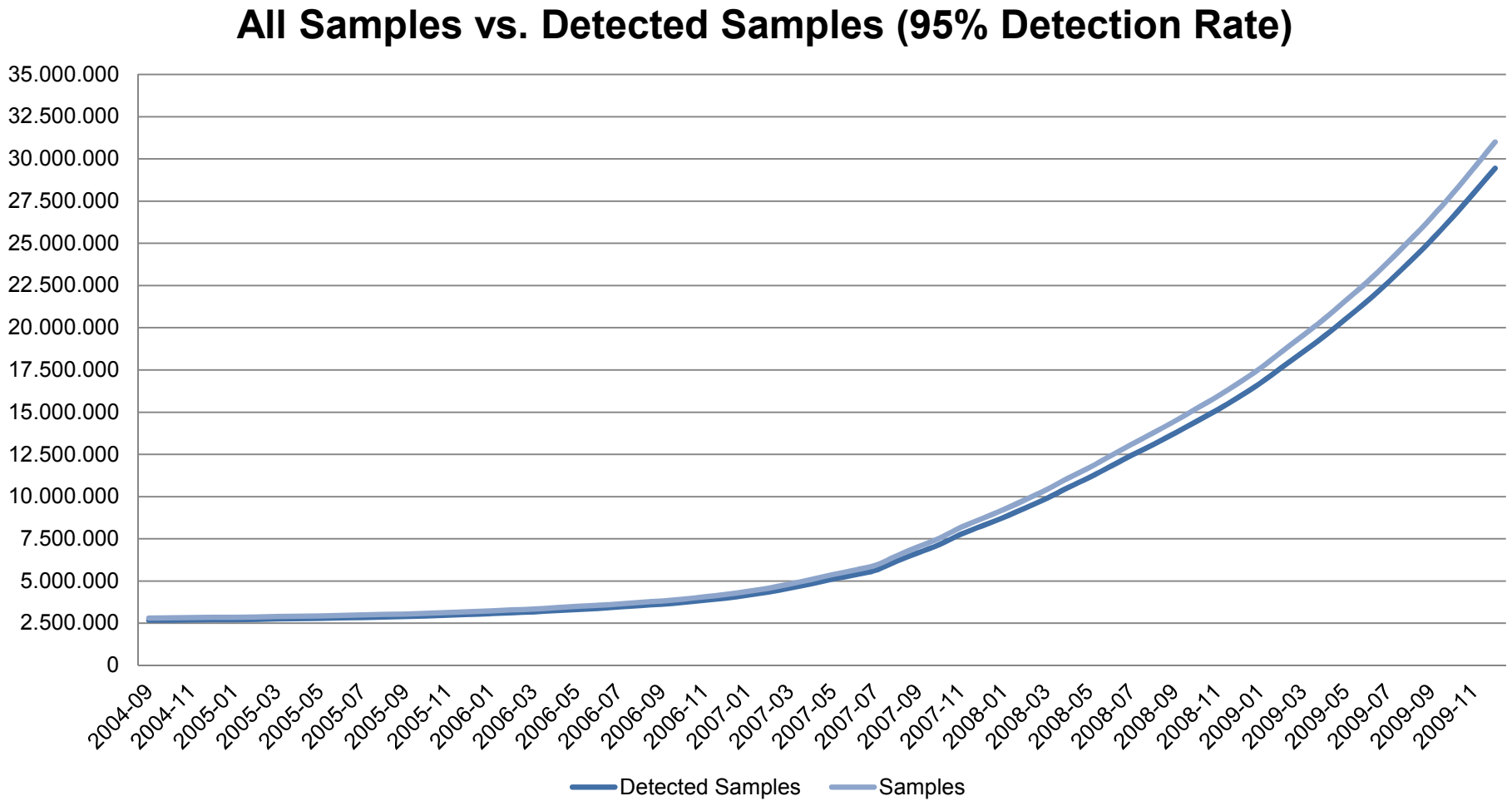
A Typical Day in Anti-Malware Industry



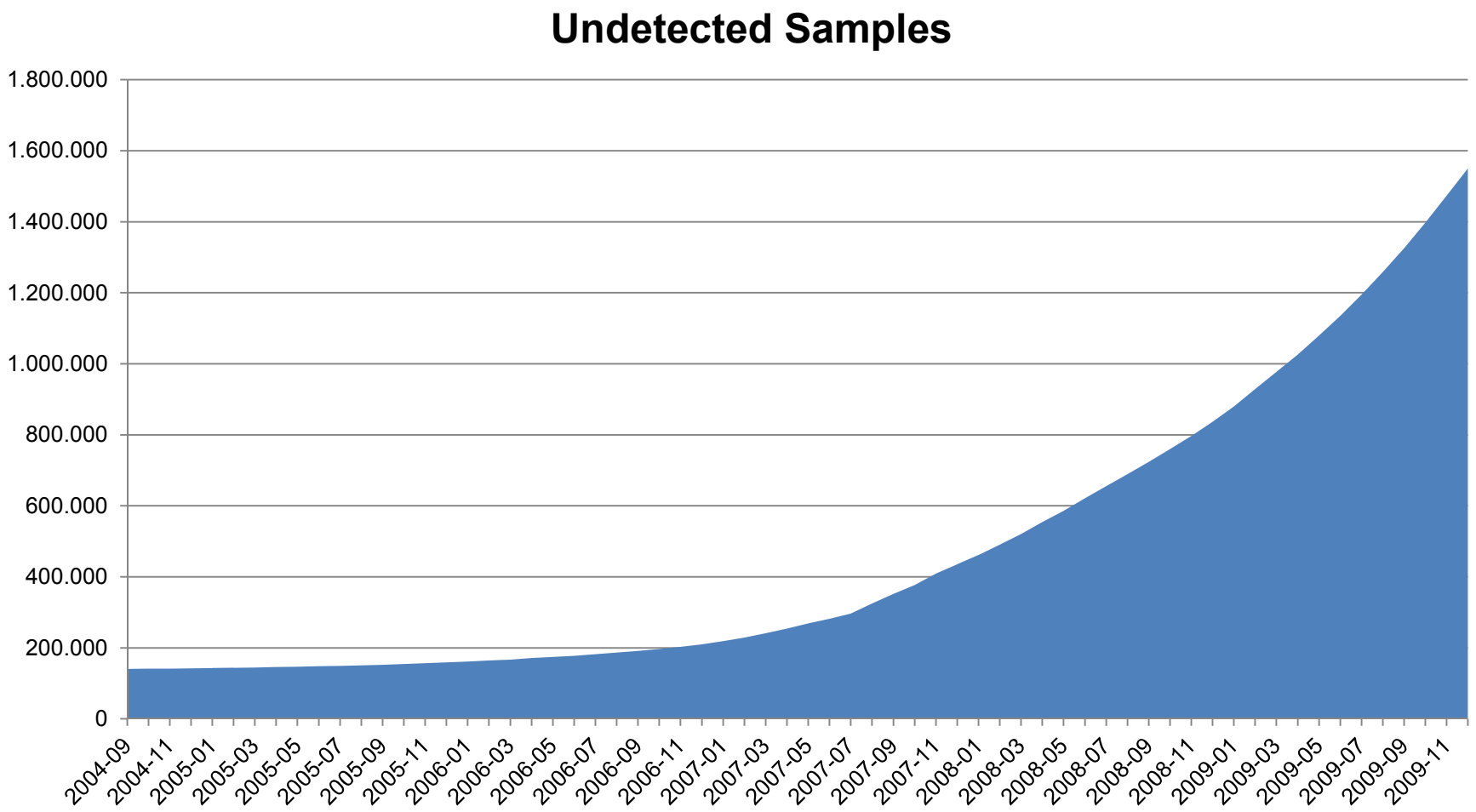
Implications

- Summary of the above
  - More and more malware is released
  - More and more signatures are provided
  - More and more updates are released
  - … and the updates are getting bigger
  - Programs are getting bigger
  - (Relative) Detection rates remain the same

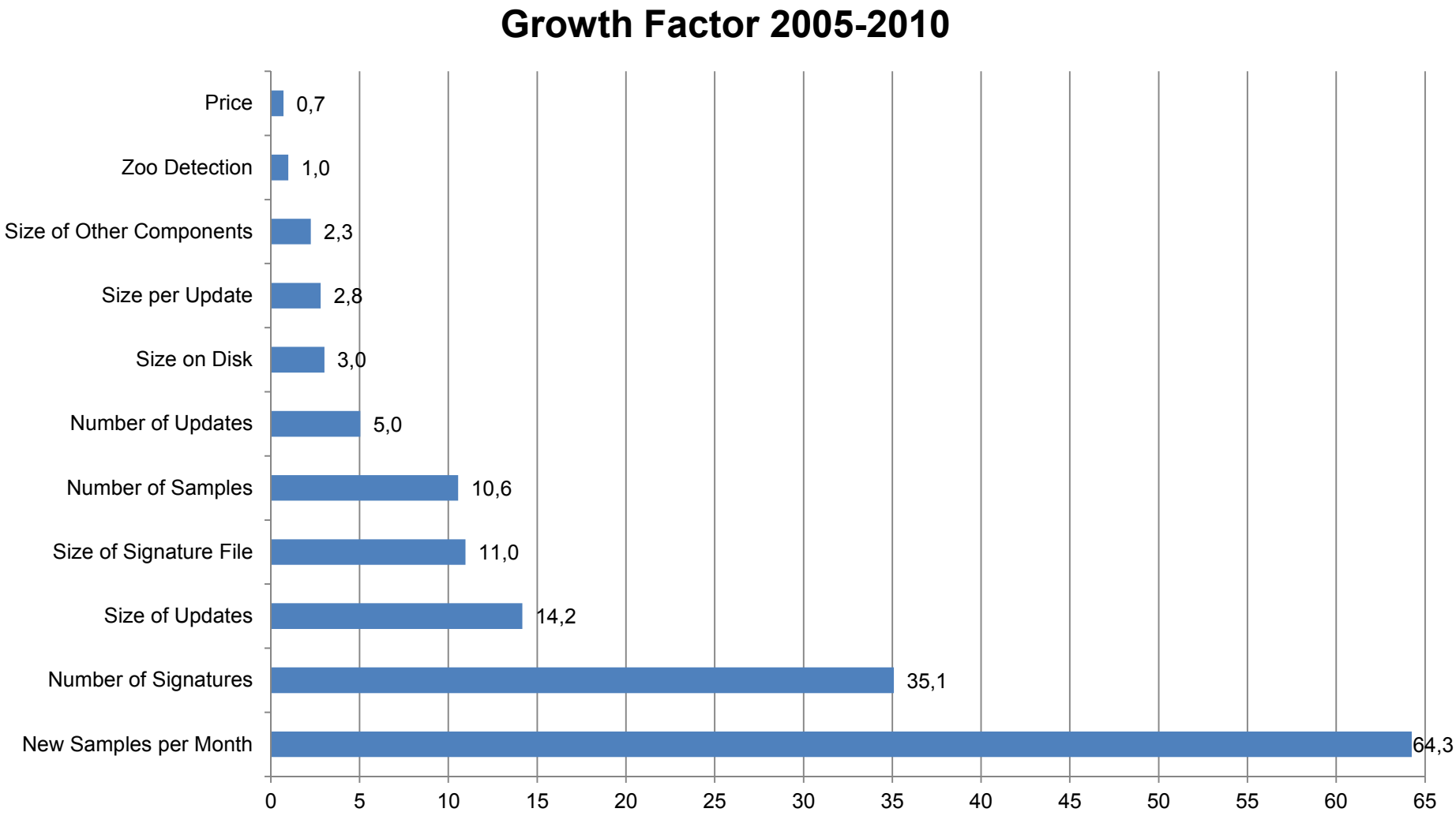
Implications



Implications

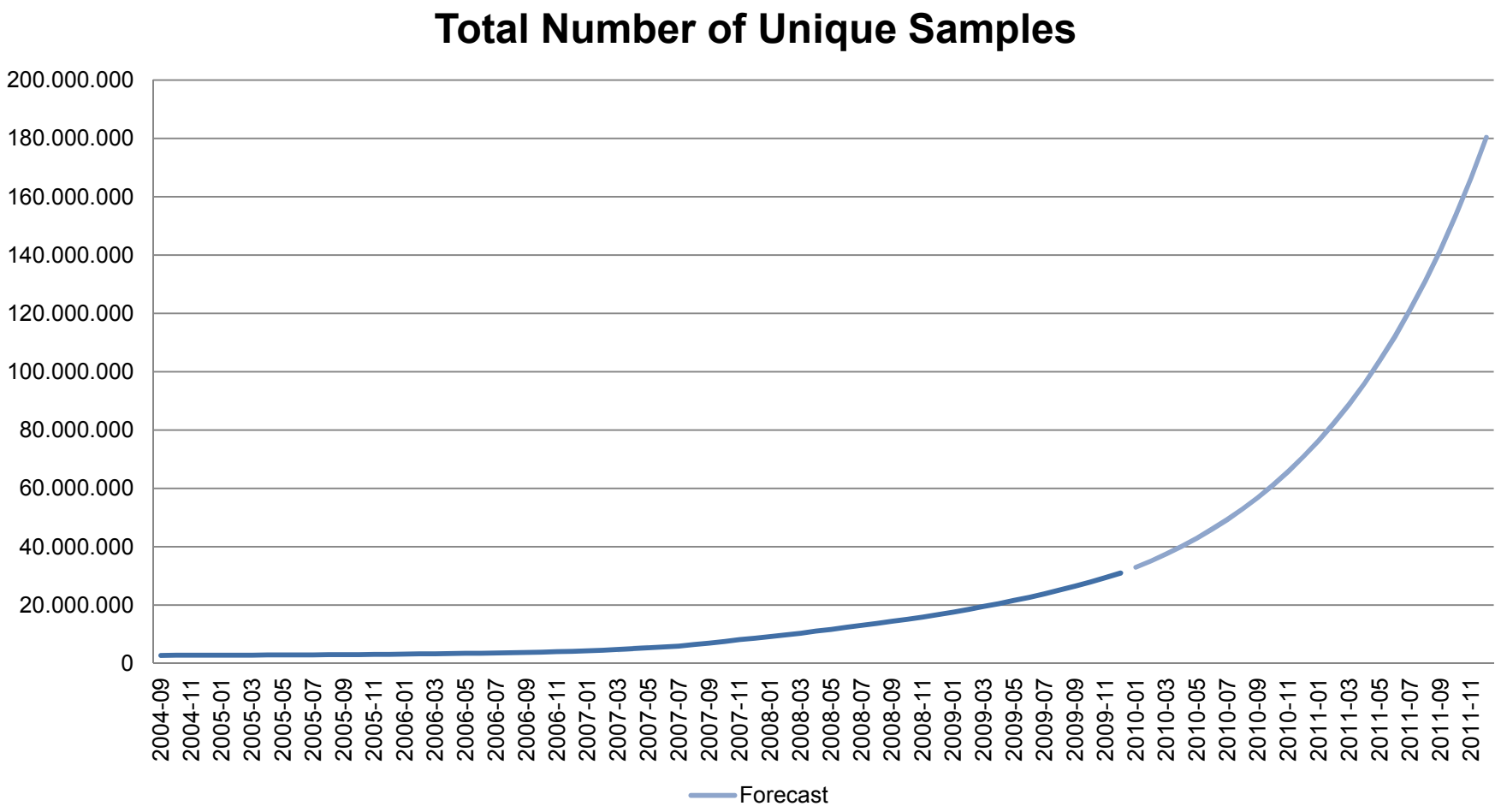


Implications



AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

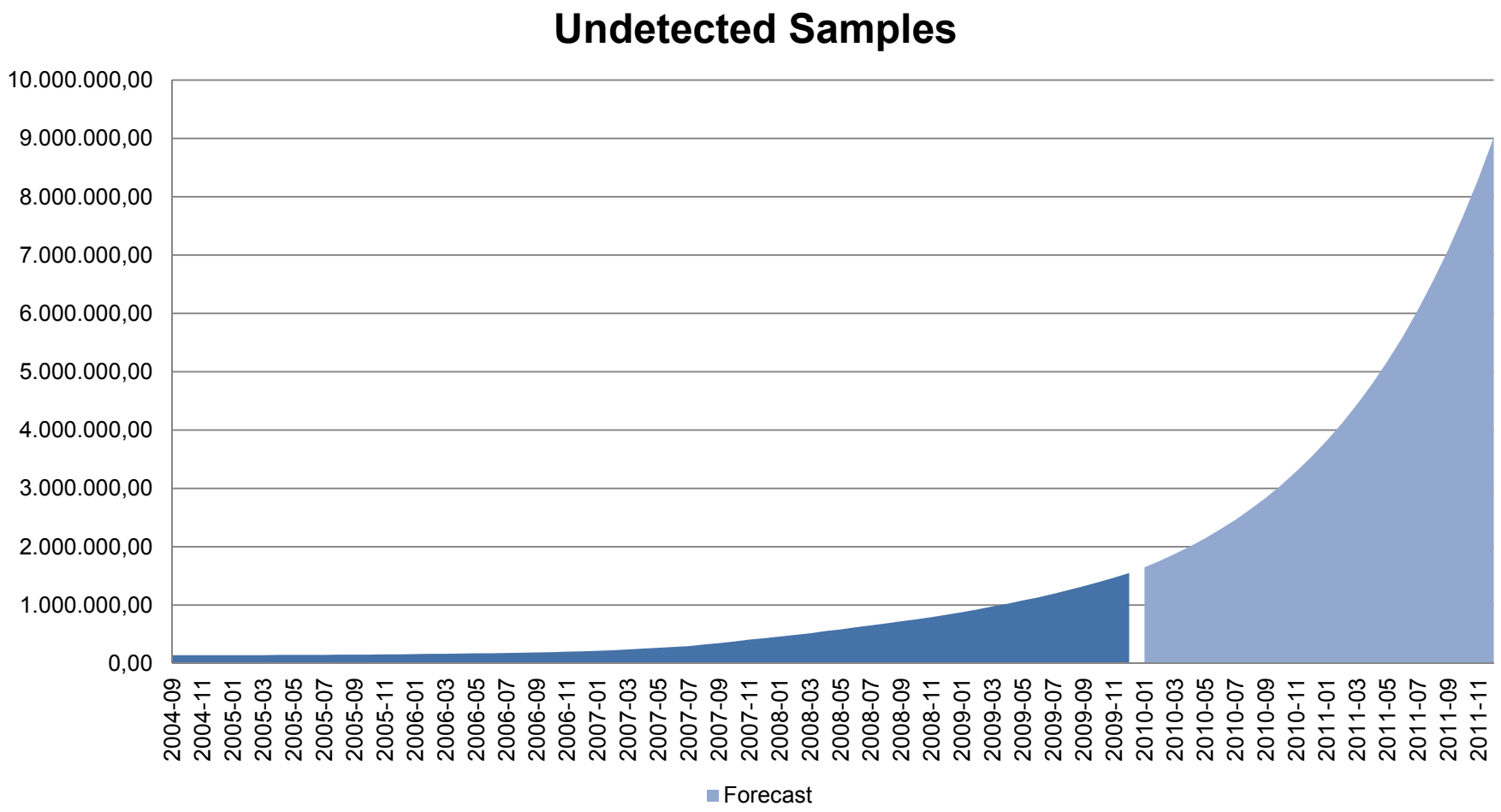
Implications



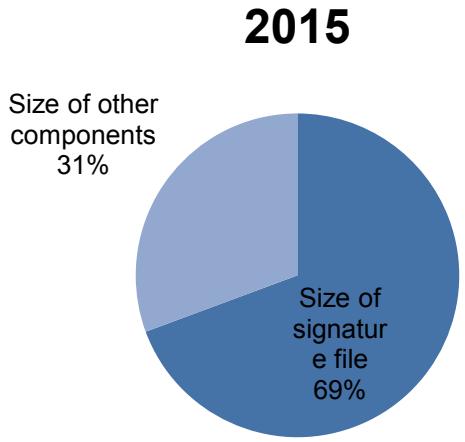
Implications

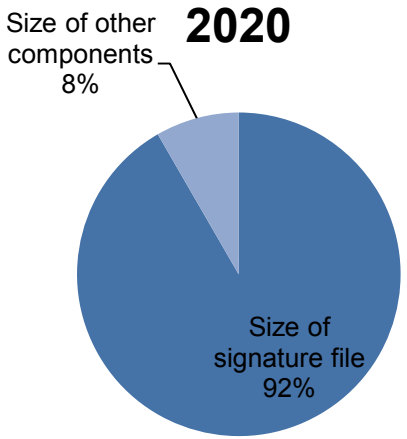
What if the problems are tackled as before?

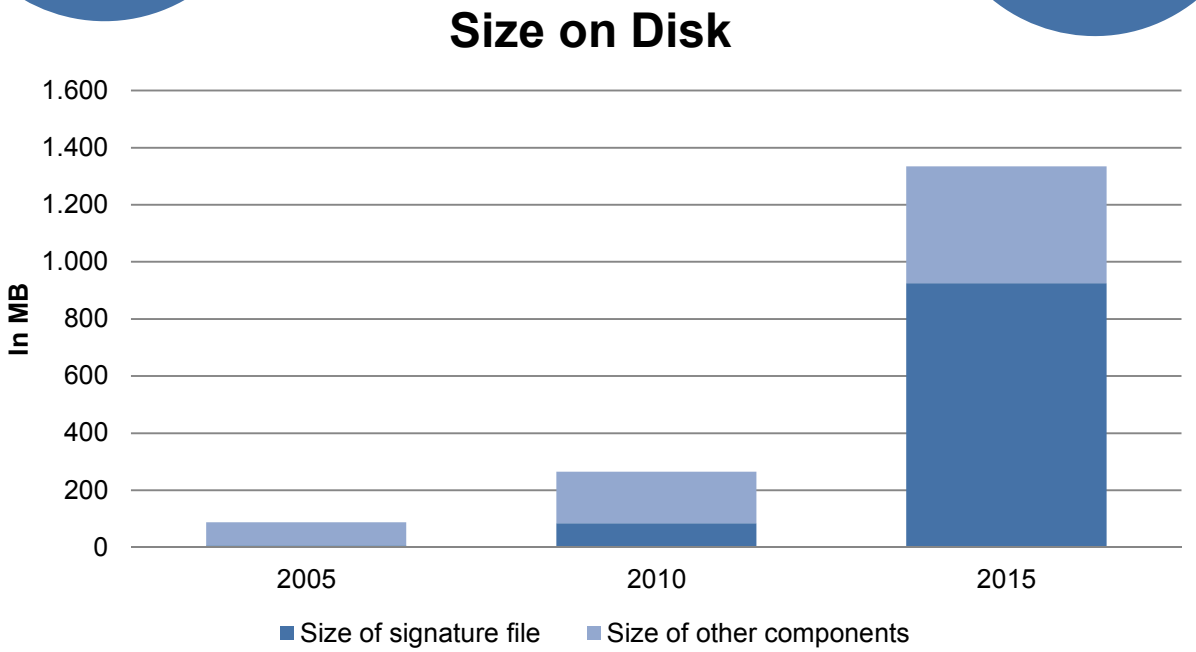
Implications



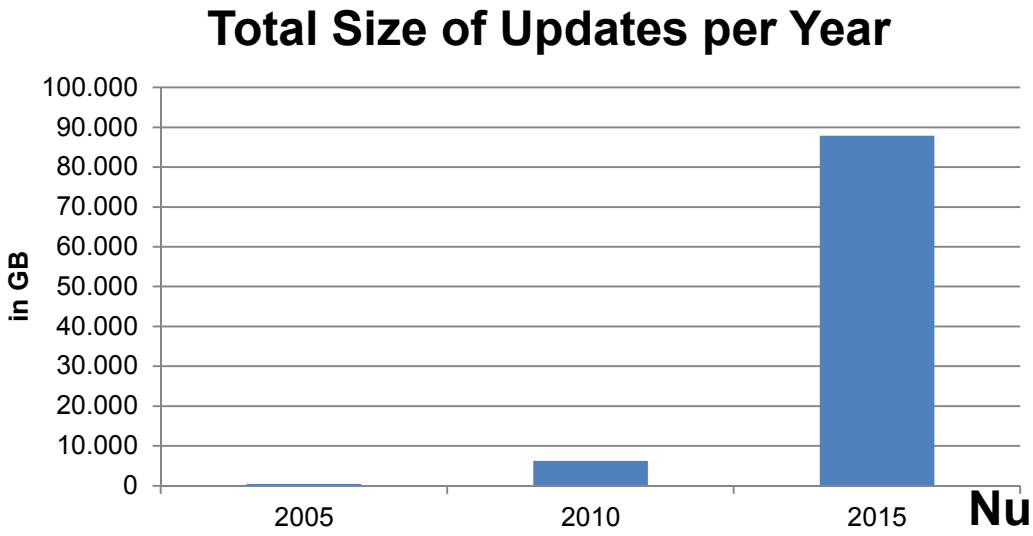
Implications

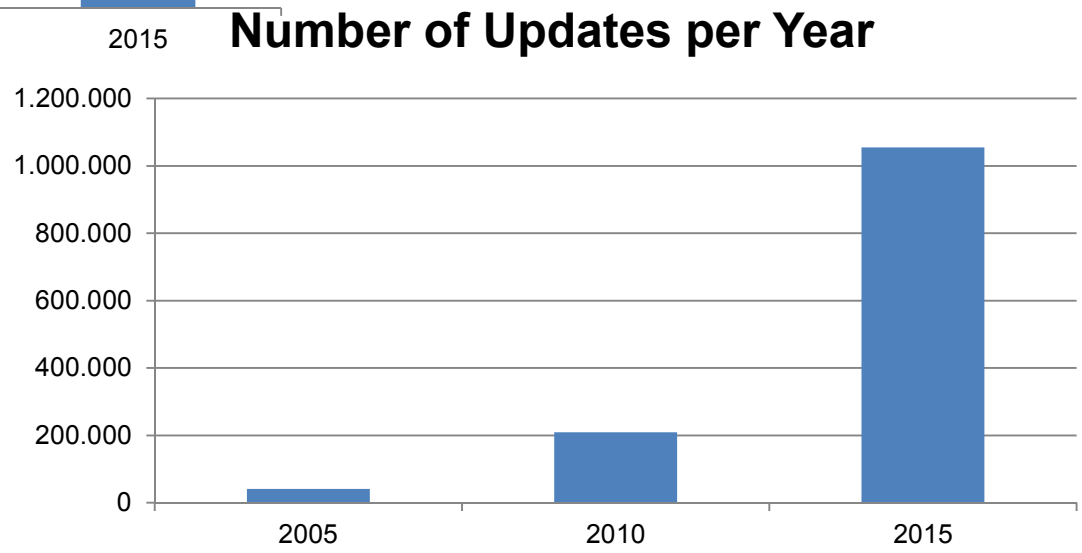






Implications





Implications

- Fortunately the Anti-Malware Industry is much more innovative then just making everything bigger on the client …

- … instead they make everything bigger and move it from the client to the cloud

- And from time to time they develop new approaches to detect malware

Implications

- What else can be concluded from the numbers above?
- Your customers get a lot more value on 2010 than they did in 2005!
- How is that?

Implications

	2005	2010
Signatures / €	2.322	114.590
Program Size / €	1,95 MB	8,29 MB
Updates / € (per year)	16	68
Size of Signaturefile / €	0,17 MB	2,63 MB
Detections / €	62.011	920.325
Features	Detect Malware	Detect Malware … and numerous invaluable additional features

Conclusions

- There are a lot of numbers and statistics to measure, to come up with and to draw conclusions from
- Not all of them are useful
  - No product is like the average
  - Sometimes there is no causal relationship
- Those that are useful may only be useful in a limited time frame
  - Detection rates change, depending on sample set, signature database, …
- Some developments and growth rates can be estimated, many can’t
  - It is nothing more than an estimation

AV-TEST
Tests of Anti-Virus-Software independent • qualified • fast

Q&A

Thank you very much for your attention!

Questions?