ENJOY SAFER TECHNOLOGY™

The (Testing) World Turned Upside-Down

David Harley
ESET Senior Research Fellow

“Why should we from good Laws be bound?
Yet let's be content, and the times lament, you see the world turn'd upside down.” (English broadside ballad.)

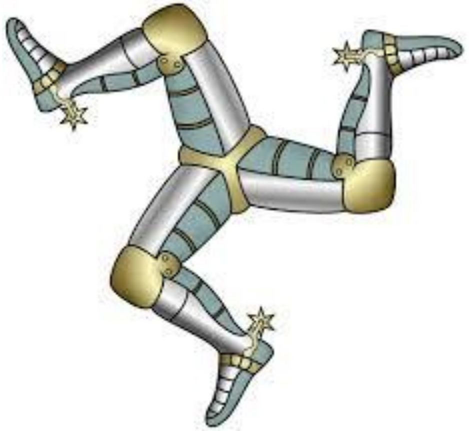
Playing Footsie

Tester

(leading foot)

Vendor

(on the back foot)



Consumer

(footsore)

Agenda

- Horrible Histories
- Test Types
- Sample Sourcing
- Aggregation Aggravation
- Simulation Exasperation
- D-I-Y Testing
- Conclusion: Forever AMTSO?

Horrible Histories

- Disabling of layers of functionality and the demotion of whole product testing
- Simulation as a comparative testing tool
- Malware creation as a means of detection testing
- Vendor-supplied test samples
- Opaque sourcing, selection, classification and validation of samples
- Promotion of D-I-Y testing as superior to independent testing.
- Pseudo-testing using resources like *VirusTotal*
- *Plus ça change…*

Test Types

- Vendors – Internal Testing
- Vendors – Commissioned Testing
- Independent Testing

Vendors – Internal Testing

- Internal Testing
  - As a strategic tool
  - As a marketing tool
- Does anyone still believe a security vendor’s marketing?

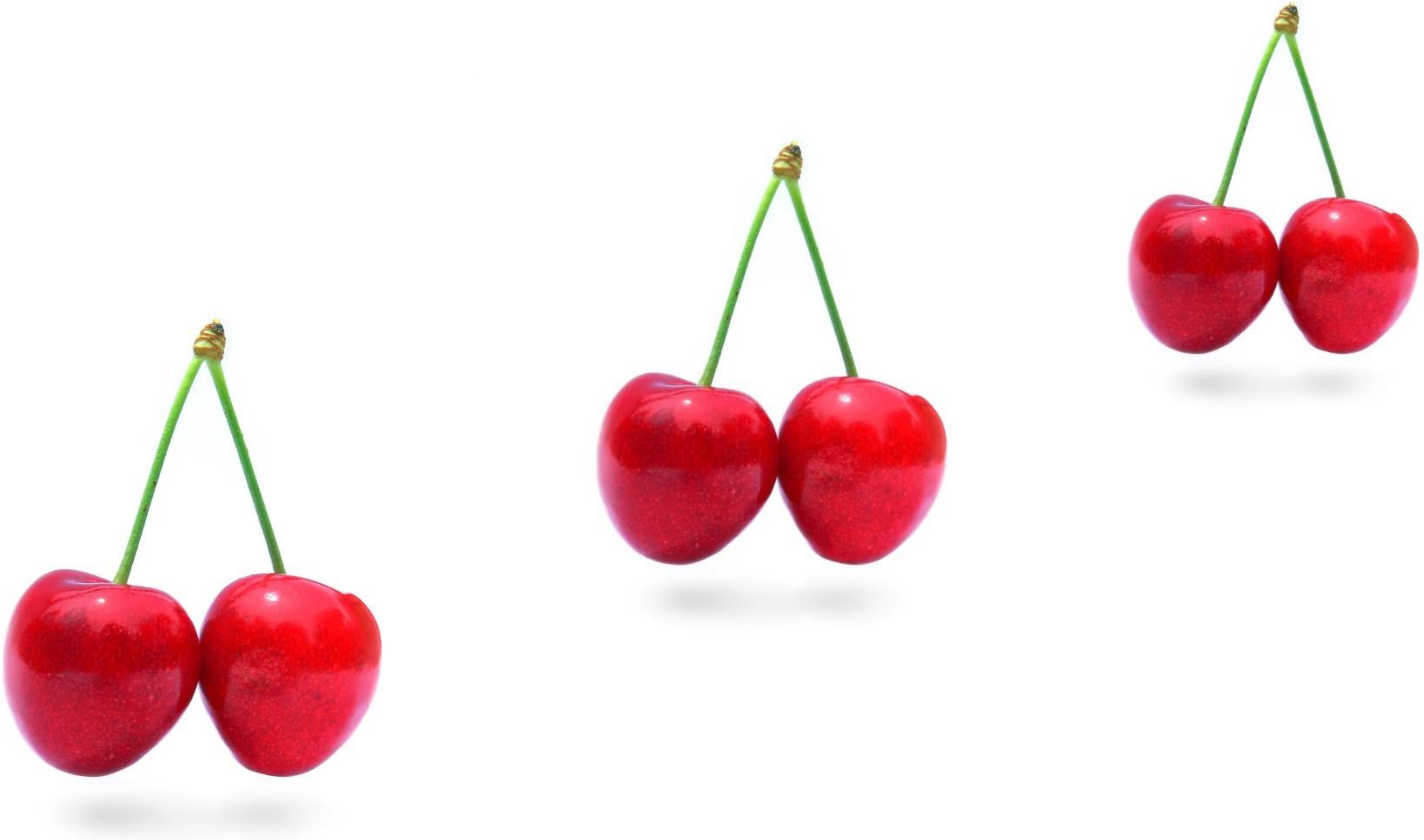
  Perceptual bias
    - Negative marketing campaigns
    - Halo effect.
    - Selective retention

  Helped along by:
    - Buzzword buzziness
    - Self-Distancing

Vendors – Commissioned Testing

- Truly independent?
  - Transparency
  - Influence over design and methodology
- Truly competent?

Conclusions from Cherry-Picked Data



Benjamint444, edited by Fir0002 - Own work CC BY-SA 3.0

Independent Testing

- Expert reviews
- In-house customer reviews
- D-I-Y reviews

Sample Sourcing

Where do independent testers get their samples?

- Their own honeytraps etc.
- Samples shared between security organizations (vendors, testers, VirusTotal et al.)
- Comparatively small communal repositories of verified malware
- Directly or indirectly from a vendor whose product is under test.

Samples from Unknown (or possibly biased) Sources

- If you use someone else’s methodology, they’re more in control than you are.
- If you rely on samples from unknown sources, the source is controlling the test.
- If the source is a vendor whose product is under test:
    - He can’t give you samples he doesn’t have
    - He probably won’t give you anything he can’t detect
    - He may be tempted to give you samples he knows other vendors won’t detect.

Thanks for Sharing

- …or not sharing…
- Oops, where did it go?
- Fresh off the production line
- Malware? What malware?
- Validated or not validated?

Simulation Exasperation

“Don’t use viruses at all. Use simulated viruses. Assume that the simulation is perfect and that therefore all products should detect them.”

(Article in Virus News International)

Simulation:

- “…rewards the product that incorrectly reports a non-virus as infected.
- “…penalizes a product that correctly recognizes the non-virus as not infected.’

(Open letter from Joe Wells and a lot of people who may even be here this week.)

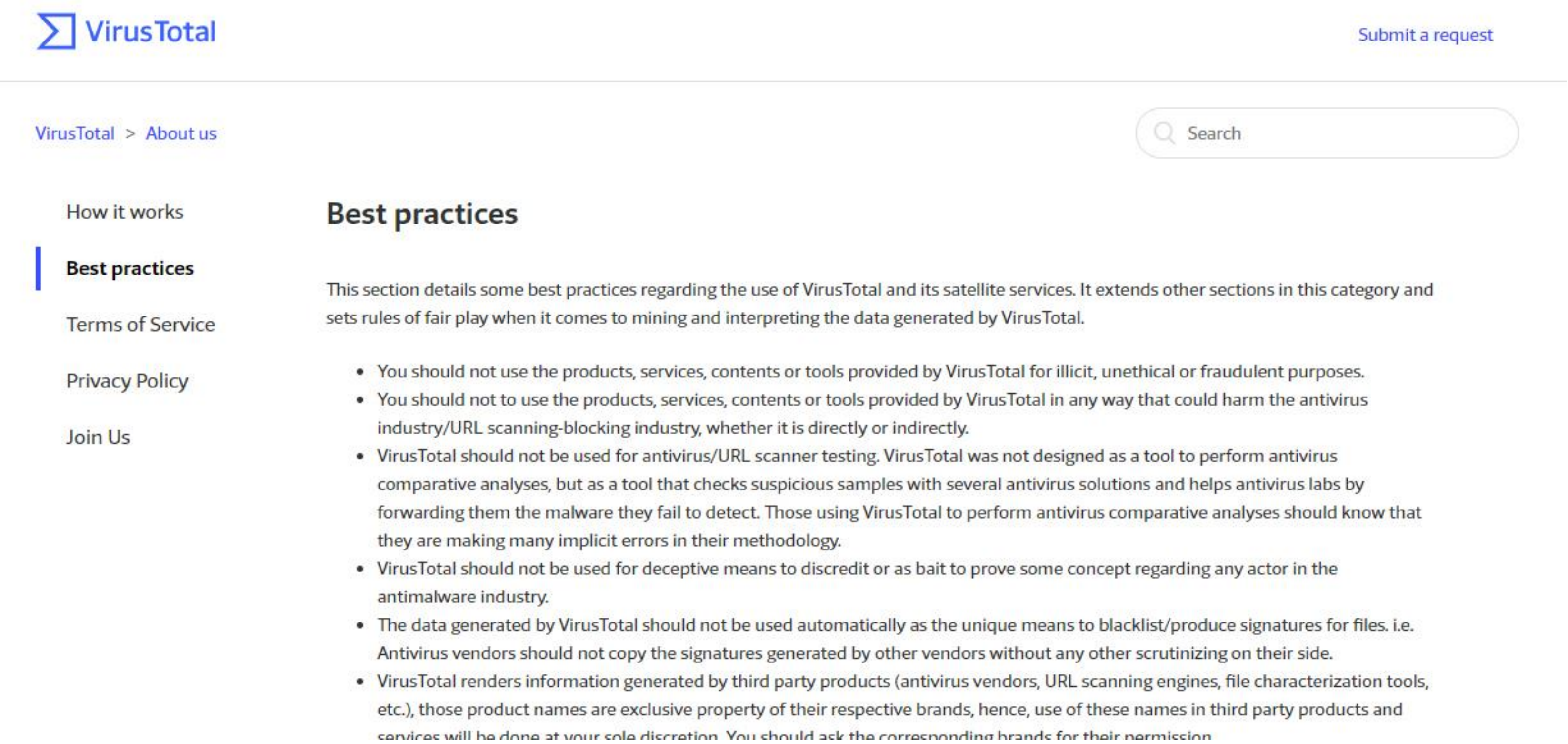
Simulation versus Attack

A simulated attack is not, by definition, a real attack, even if it's a *good* simulation.

Which isn't generally the case.

(This is a simulated tiger, and not suitable for tiger-detection purposes.)

Multiscanner Misuse



Best practices

This section details some best practices regarding the use of VirusTotal and its satellite services. It extends other sections in this category and sets rules of fair play when it comes to mining and interpreting the data generated by VirusTotal.

- You should not use the products, services, contents or tools provided by VirusTotal for illicit, unethical or fraudulent purposes.
- You should not to use the products, services, contents or tools provided by VirusTotal in any way that could harm the antivirus industry/URL scanning-blocking industry, whether it is directly or indirectly.
- VirusTotal should not be used for antivirus/URL scanner testing. VirusTotal was not designed as a tool to perform antivirus comparative analyses, but as a tool that checks suspicious samples with several antivirus solutions and helps antivirus labs by forwarding them the malware they fail to detect. Those using VirusTotal to perform antivirus comparative analyses should know that they are making many implicit errors in their methodology.
- VirusTotal should not be used for deceptive means to discredit or as bait to prove some concept regarding any actor in the antimalware industry.
- The data generated by VirusTotal should not be used automatically as the unique means to blacklist/produce signatures for files. i.e. Antivirus vendors should not copy the signatures generated by other vendors without any other scrutinizing on their side.
- VirusTotal renders information generated by third party products (antivirus vendors, URL scanning engines, file characterization tools, etc.), those product names are exclusive property of their respective brands, hence, use of these names in third party products and services will be done at your sole discretion. You should ask the corresponding brands for their permission.

Aggregation Aggravation

Aggregation

(Re-)Interpretation of data

Misrepresentation & Certification

Who Pays the Piper?

Forever ~~Amber~~ AMTSO?

AMTSO principle	Text of principle
1	Testing must not endanger the public.
2	Testing must be unbiased.
3	Testing should be reasonably open and transparent.
4	The effectiveness and performance of anti-malware products must be measured in a balanced way.
5	Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.
6	Testing methodology must be consistent with the testing purpose.
7	The conclusions of a test must be based on the test results.
8	Test results should be statistically valid.
9	Vendors, testers and publishers must have an active contact point for testing related correspondence. [The phrase 'testing related' is probably meant to be 'testing-related'.]

AMTSO – still in with a chance?

- More conversation, less litigation
- Vendors and accountability
- Testers and accountability

Conformance to expertly formulated and agreed standards and guidelines

- Transparency of affiliations and methodology
- Reproducibility of results and methodology
- Statistical accuracy based on sound metrics:
  - sample set rightsizing
  - sampling techniques
  - metrication and instrumentation
  - realistic and accurate analysis
  - bias exclusion

Pain Points

- Pay to Play
- Licensing disagreements
- Involuntary participation
- Misrepresentation of test results
- Methodological disagreements

Ethical grounding, objective validity

- Responsible disclosure
- Declaration of interest
- Responsible sample sharing
- Duty of care (safety)
- Clarity, and avoidance of misleading statements and conclusions
- Methodological validity based on:
  - comparing apples to apples rather than melons to grapes
  - consistency of test objectives with stated purpose
  - selection of appropriate test scenarios and samples sets

If summer were spring and the other way round, Then all the world would be upside down. (Trad.)

ENJOY SAFER TECHNOLOGY™

And now, over to you...

David Harley

ESET Senior Research Fellow

David.Harley.IC@eset.com

www.eset.com | www.welivesecurity.com