COMMENTARY

ANTI-VIRUS: LAST RITES, OR RITES OF PASSAGE?

David Harley
ESET, UK

Anti-virus is dead. Again. Actually, the corpse has been walking and talking for so long that it's a wonder no one has called Buffy Summers [1] to put a stake through its heart. However, one of our competitors did summon the spirit of *VirusTotal* (*VT*) to prove that AV is so far past its best-before date that it should only be used when given away free [2] (or maybe retrieved from the dustbins at the back of the cybermarket) .

The quasi-test – implemented by ignoring *VT*'s own recommendations and commentary on the misuse and misrepresentation of the service as a substitute for comparative testing [3] – actually tells us very little about real detection rates for the samples that were used, even assuming that they were valid samples of unequivocally malicious software. As *VT* rightly states: 'Those who use *VirusTotal* to perform anti-virus comparative analyses should know that they are making many implicit errors in their methodology.' I'll explain what some of those errors are later, but let's assume for the moment that *VT* is just being modest, and that a *VT* report is an accurate reflection of a product's detection performance (it isn't, and isn't meant to be).

At a time when AV labs process hundreds of thousands of samples a day, to claim on the evidence of 82 unverified samples that 'Anti-virus software is now so ineffective at detecting new malware threats most enterprises are probably wasting their money buying it' has more to do with marketing than with statistics. Since, by definition, we can't say what figure '100%' of known and unknown malware represents at any moment in time, we can't say what percentage of that totality is *detected* at any moment in time by any single AV product, let alone *all* products. We do know, though, that a very significant proportion of new threats are detected as soon as they appear by some form of code analysis and/or behaviour analysis. Of course, it's nowhere near 100%, or even the 80% that some AV vendors claimed for heuristics in the 1990s, and no AV researcher worth listening to would claim that it *is*, but it's a lot more than 0%.

If there's *any* single security solution (not just AV) that offers 100% detection and/or blocking of all malware and is easy and convenient to use, totally transparent to all business processes, and never generates any form of false positive, I wish someone would tell me what it is so I can go and buy a copy.

If this were a real test, I'd be sceptical of its accuracy because I don't know how the results were validated. We have no idea what samples were used (apparently acquired via TOR) or whether they were correctly classified as malware, still less about their prevalence. In the absence of that information, and of real testing that checks detection of validated samples against the whole functionality of the product (or at least both on-demand and on-access scanning) and using like-for-like configuration, there is more than a whiff of marketing about this exercise. Quasi-testing with *VirusTotal* is never going to accord with AMTSO's basic principles of testing [4] unless *VT* drastically re-engineers its mechanisms and objectives.

The fact is, *VT* was never intended as a mechanism for testing AV, and that is made very clear. A *VirusTotal* report doesn't tell you which solutions *know* about a specific threat sample. It tells you which (if any) solutions will flag it as a threat under very restricted conditions that don't reflect real-world conditions. If *VirusTotal was* meant as a tool (or a substitute) for comparative testing, it would be a very bad one.

But that isn't its purpose at all: it's meant to provide some idea as to whether a submitted file is malicious. (Even then the answer is equivocal: if enough vendors tell you it's malicious, the chances are it is, but if no vendor flags it as malicious, that doesn't mean it *isn't* malware.) *VirusTotal* is what it is – not a parable, but if you insist on describing it with an analogy, it's more like a heuristic scanner than a comparative test. A scanner with a tiny heuristic rule-set:

(Rule 1)

IF

One or more scanners flag file X as malicious or suspicious

THEN

File X is definitely suspicious (but not proven malicious)

(Rule 2)

IF

No scanners flag file X as malicious or suspicious

THEN

File X is not suspicious (but could be malicious and undetected)

OK, I'm being a little disingenuous here: *VirusTotal* does a lot more than that (and its full range of services is highly appreciated by the AV industry), but that's the functionality that is being cited by quasi-testers. (*VT*'s Julio Canto and I put together a paper [5] and presentation a couple of years ago for my favourite forensics conference [6] that covers what *VT* does in some detail, but also specifically addresses the issue of quasi-testing.)

VirusTotal is unsuitable for comparing product detection performance because the products it uses cover a wide

range of functionality, and it doesn't configure all products to the same level of paranoia, or exercise all the layers of functionality they may comprise.

This means, for instance, that some products will flag potentially unwanted applications (PUAs) as malware: on some products, this is because of default settings, and in other cases, because *VT* has been asked by the vendor to turn on a non-default option. In other words, some products as configured by *VT* may never detect certain samples because they're not unequivocally malicious. If *VT* was a test, it would be more a test of vendor philosophy in terms of configuration parameters than a test of objective detection capability.

Other products may be able to detect a given sample on access, but not on demand, because not all approaches to behaviour analysis and heuristics can be implemented in static/passive scanning. *VirusTotal* uses command-line versions, and those versions do not implement whole product functionality because of the limited execution context of an essentially non-interactive scanner. To summarize the conclusion from that CFET paper [5]:

> *VirusTotal is a highly collaborative enterprise, allowing the industry and users to help each other. As with any other tool (especially other public multi-scanner sites), it's better suited to some contexts than others. It can be used for useful research or can be misused for purposes for which it was never intended, and the reader must have a minimum of knowledge and understanding to interpret the results correctly.*

Heuristics, generic detection, cloud technology: the AV industry has continuously attempted to adapt to changes in malicious technology and accelerating volumes of malware. What it hasn't done is communicate the extent to which anti-virus has ceased to be the product that it was decades ago – largely focused on detecting known virus samples (though even then, many products also had bundled integrity checkers, basically a form of whitelisting) – and has become a multi-layered product in its own right, incorporating several layers of defence. But anti-virus is not enough by itself, which is why mainstream products now incorporate their AV functionality into security suites. Sadly, they're not enough either, but then I'm not holding my breath waiting for a one-size-fits-all, never-needs-updating, 100% effective, never-gets-in-the-way-of-a-legitimate-process solution.

In principle, reputable security mavens advocate a sound combination of defensive layers rather than the substitution of one non-panacea for another. Actually, a modern anti-virus solution is already a compromise between malware-specific and generic detection, but I still wouldn't advocate anti-virus as a sole solution, any more than I would IPS, or whitelisting, or a firewall.

While some competitors in other industry sectors stop short of saying that people shouldn't use AV, they often suggest that there is no need to pay for it.

Vendors and journalists are actually doing their users/readers a disservice by suggesting that companies should use free AV so as to be able to afford another panacea du jour – not only because:

- that advice ignores the licensing stipulations that usually govern the legitimate use of free versions of commercial products;
- free AV has restricted functionality and support, especially when it's primarily a loss leader – a trailer to the main (for-fee) event;
- free AV has to make some other return on investment, which may take the form of strings attached in the form of complementary utilities, even adware [7].

Rather, because even if they're the only security software in use, security suites offer more comprehensive, multi-layered protection than a product (free or otherwise) that only offers one layer of protection.

But can we imagine a world without AV, since apparently the last rites are being read already? A world in which vulnerability researchers get paid, but AV researchers don't, isn't altogether a pleasant prospect. While many of us do or have done a certain amount of *pro bono* work (in education and awareness raising, in standards organizations, and so on), most of us have to work for a living. It's unlikely that free AV would survive except among enthusiastic amateurs and companies in other security sectors throwing it in as a value-add, like those *Mac* utility vendors in the 90s who included detection of the few *Mac* viruses that existed at that time. Would the same companies currently dissing AV while piggybacking its research be able to match the expertise of the people currently working in anti-malware labs?

REFERENCES

[1] http://en.wikipedia.org/wiki/Buffy_the_Vampire_Slayer_%28TV_series%29.

[2] http://www.imperva.com/download.asp?id=324.

[3] https://www.virustotal.com/about.

[4] http://www.amtso.org/amtso---download---amtso-fundamental-principles-of-testing.html.

[5] http://go.eset.com/us/resources/white-papers/cfet2011_multiscanning_paper.pdf.

[6] http://www.canterbury.ac.uk/social-applied-sciences/computing/conferences/CFET2011/Home.aspx.

[7] http://blog.eset.com/2012/12/04/why-anti-virus-is-not-a-waste-of-money.