virus BULLETIN Covering the global threat landscape

HYPE HEURISTICS, SIGNATURES AND THE DEATH OF AV (AGAIN)

David Harley
ESET

I was first told that viruses weren't a problem way back in the 90s, long before I was assimilated by the security industry. Notably 'because operating systems are becoming so secure'. Providers of operating systems can certainly claim that *Windows NT* and its offspring; *OS X*; *iOS* and *Android* have all played a part in the near-extinction of 'proper' viruses, though none of them should be claiming to have eliminated the problem of malware, of which viruses now constitute a tiny proportion.

EXPECTATION MANAGEMENT

No less a person than Alan Paller of *SANS* once said to me something to the effect of 'Are there such things as viruses?' (in 1997, I think). I believe he meant *not* to suggest that viruses were an urban legend (as Peter Norton had, even earlier in the history of computer security, and before his name became linked with a well-known anti-virus product) but that they were really not worthy of much consideration by the 'real' security industry.

Perhaps it's unfair to take issue with a throwaway remark made at a conference reception several years ago, but in spite of the many useful things *SANS* has done in the security field (some of them with reference to malware analysis), the organization does have a history of a poor understanding of some of the issues relating to malware. A couple of instances spring to mind: the distribution of trivially modified malware code [1], and the assertion (again by Alan Paller) that methodologically-challenged testing by *Consumer Reports* [2] was 'fair and rigorous' [3]. In that latter communication (in a *SANS* newsletter [4]), Paller also commented:

> '…the leading AV companies… have traditionally not done well in finding and blocking new viruses quickly. But for goodness sakes, if they don't do well at finding and blocking new viruses, why are we buying them?'

Unfortunately, the debate on the value of anti-malware (and what should be expected of it) doesn't seem to have died any more than the malware detection industry has. In fact, it probably hasn't escaped your notice that press releases about the death (or at any rate the essential uselessness) of anti-virus (never, somehow, anti-malware) tend to coincide with major media-friendly events such as *RSA* and *Infosecurity*. (Or that they tend to originate with security companies who seem to take it personally [5] that money that should be going to them is being diverted to the 'should-be-extinct' anti-virus industry [6].)

SECURITY, JOURNALISM AND SCHADENFREUDE

Of course, we've also learned to expect the media to seize gleefully on bad news relating to this industry. *The Register* never seems to miss an opportunity to bang another nail into the coffin, however tenuous the link to the story [7]. When *Google* published an interesting paper [8] contrasting the views of non-experts and self-defined security experts on the most critical security practices, the top-of-the-article takeaway message from *El Reg* [9] was 'Antivirus software has copped another beating from security experts'. However, the fact that 'non-experts' were likelier than 'experts' to put the use of anti-virus near the top of their list of must-do security measures was a rather minor aspect of the paper. But it seems that knocking the AV industry still takes second place at *The Register* to knocking the NHS, so perhaps my move away from health care to security in 2006 was still the right direction. As I said in an (unanswered) comment to an article with the wonderfully alarming title 'NHS XP patch scratch leaves patient records wide open to HACKERS' [10]:

> 'I'm disappointed to find myself quoted in an article with such a sensationalist, misleading, NHS-bashing title. It's not, of course, impossible that patient records are exposed to hacker activity… I was asked for and commented regarding hypothetical scenarios, and am not happy to find that my comments have been used to support the assertion that patient records are at risk. The fact is, I don't know if that's the case, and I suspect *The Register* doesn't either…'

But I digress. Of course, *The Register* isn't the only news source to enjoy a little anti-malware-related controversy. The last time I went to an *Infosecurity Europe* event (in 2014), *Infosecurity Magazine* was still running a head-to-head pair of mini-articles by myself [11] and Ryan W. Smith [12], meant to represent pro and con 'counterpoints' regarding anti-virus ('Anti-virus: Art Thou Dead?'). I suspect that I'm something of a disappointment in debates like this (debate not really being the right word, as we didn't get to see each other's articles until they were published), since I always take the position that anti-virus as it was when I was first sucked into this game is indeed an ex-parrot [13], as it *should* be. In this instance, I suspect the shock value of the argument was even less. While 'AV: Little More Than a Team Player' [12] sounds more than a little dismissive, the first and last paragraphs of Smith's article say nothing that I might not have said myself: anti-virus is not enough [6], and multi-layered security [14] is the way to go.

AV IN A&E

In fact, there's quite a lot in that article I agree with; unfortunately, it's significantly misleading because Smith, like so many others, seems to think that (a) anti-virus is locked into the model of detection by static signature of the late 80s/very early 90s, and (b) it only detects malware (though that's an improvement on those commentators who believe we only detect viruses). In fact, there's very little in his vision of a layered approach to security that isn't addressed at least partially by modern detection-oriented security suites, and even 'simple' anti-virus usually detects much more than 'real' viruses and goes far beyond static signatures in detection methodologies.

This isn't meant to be a treatise on anti-malware technology – many of you will know more about that than I do – so I'll just point out in passing that detection of malware is basically an application of heuristic analysis (yes, even the most elementary signature detection is an example of a heuristic). Not just the elementary passive heuristics of the early 90s, but the more advanced, active behaviour analysis and sandboxing that other sectors of the security industry seem to think that anti-malware companies are incapable of implementing.

Here's a heuristic: if an article talks about 'the dirty little secret of anti-virus', it deserves several pinches of salt. Consider, for example, the stampede of journalists who (partially or completely) bought into *Imperva*'s methodologically suspect attempt to prove that 87% = 5% [15] when discussing anti-malware detection rates. A recent article by Corey Nachreiner in *(IN)SECURE* [16] uses the same cliché – 'Signature antivirus' dirty little secret' – but does at least admit that 'antivirus was, and still is, a valuable addition to your layered security strategy'. However, the article then goes on to explain:

> 'After hearing legacy AV is that bad, you may wonder what you can do. Behavioural malware detection, sometimes called next-generation sandboxing, is the solution.'

Isn't that one of the approaches anti-malware apps have been taking for years? Apparently not:

> 'Signature-based AV can't keep up and fails to catch the latest malware on a regular basis. Behavioral or heuristics-based malware detection helps, but basic implementations found in host-based solutions are only partially effective. If you really want to protect from today's highly evasive, constantly morphing threats, I highly recommend you add an advanced malware detection or next-generation sandbox solution to your existing layers of defense.'

As my pseudonymous ex-colleague Mac Bloggit implies [15], there is a basic misunderstanding or even misrepresentation in articles that talk about the anti-malware industry as if it were locked into a reactive signature detection model, ignoring 'the terms heuristic analysis, behaviour blocking, sandboxing, behaviour analysis, whitelisting, integrity checking, traffic analysis, and emulation,' or even misrepresenting them as unique to their own product sector.

SIGNATURE DISH

In fact, a second heuristic might be to mistrust any article that talks about anti-virus signatures.

As Mac Bloggit remarks, with commendable restraint:

> 'Not that all AV scanners use all these techniques, but to suggest that AV is totally dependent on static signatures is at best clueless.'

And what excuse is there for allegedly IT-savvy journalists who swallow these misleading statements uncritically? Consider, for instance, this quote from the *New York Times* [17]:

> 'Part of the problem is that antivirus products are inherently reactive. Just as medical researchers have to study a virus before they can create a vaccine, antivirus makers must capture a computer virus, take it apart and identify its "signature" – unique signs in its code – before they can write a program that removes it.'

DIRT AND BRICK DUST

Excuse me while I take a short break to wipe brick dust from my forehead.

There are (at least) two problems with this 'dirty little secret':

- The anti-malware industry is no 'dirtier' than all the other security industry players who've somehow failed to eliminate computer crime completely.
- Even when anti-malware was still (more accurately) called anti-virus and detection rates were, proportionally speaking, far higher than they are today, the AV research community was warning against reliance on the black-listing approach to pre-identified malware. Even as both malware and anti-malware technology has become more diverse and more sophisticated, high-profile anti-malware researchers have emphasized key points such as:
  - Malware detection hasn't been confined to simple string matching for decades.
  - Blacklisting malicious applications doesn't catch everything.
  - Even more generic approaches to detection don't catch everything.
  - There is no 100% solution, and multi-layered security gets far closer to 100% than single point solutions.

In other words, guys, *it isn't dirty or a secret!*

Or is it?

WE NEED TO TALK ABOUT KEVIN

The resolutely independent security sceptic Kevin Townsend (I contribute regularly to his *IT Security* UK blog site) is largely concerned in his article 'The anti-virus industry does itself no favours' [18] about his lingering suspicions that 'the anti-virus industry is maybe not so clean from NSA taint as it should be'. That's an interesting and complex topic [19] for another time, but one point he makes is certainly worth addressing here:

Either AV turns a blind eye to certain problems (hence the lingering doubts), *or* AV is simply not as good as it pretends.

Kevin claims that:

> 'The industry continually publishes test results proving that it stops 99.9% (or more) of all malware…'

Certainly vendors are fond of publishing test results that favour their products, but I don't know if anti-malware vendors are still making such sweeping claims. I think there are two slightly different issues here.

Firstly, there is (obviously) no test that involves the use of *all* malware, or even all known malware. That would be an exercise of mammoth – galactic, even – proportions. The challenge (actually just one of the challenges [20]) for a tester is (or should be) to convince an audience that a far smaller sample set is sufficiently representative of the rest of the malware population to be the basis of a reasonably accurate assessment of product performance. (Assuming a competent methodology and so on, which isn't by any means a given.) In fact, mainstream testers have moved away from static testing with large test sets of ageing samples towards testing strategies that are based on trying to use currently active malware. Even this isn't necessarily 'truly representative', but it's several steps closer to the right direction.

THE TOAST WITH THE MOST

It would be a rash tester or vendor who claimed that good performance in any given test was a guarantee of perfect detection of all malware. Though many of us with one foot in the Jurassic will remember those TOAST claims [21] about 'The Only Anti[something] Software That…'

There was a time, of course, when the WildList was much closer to representing all *known active* viruses, but that was a long time ago, in the days when nearly all malware *was* viral. More recently, the WildList has retained some usefulness [22] as a baseline metric for certification testing, like VB100 [23], but in no way does it represent all malware or even all viruses 'in the wild.' In fact, the concept of 'in the wild' doesn't mean much more in the current threat landscape than 'what the WildList [24] says it is': basically a collection of validated samples (WildCore), and I don't think any reputable test is based purely on WildCore or even RTTL [25].

It is, of course, no bad thing if a product does well in a well-executed test, but when a product scores (nearly) 100% in a test, that shouldn't be understood or promoted as 'detects all malware'. If customers think that 100% detection of what they understand as 'all malware, known and unknown' is what they're buying, perhaps it's no wonder the industry is still so widely mistrusted [26]. And if there are still products marketed on that basis, perhaps the marketing departments concerned are doing both their companies and their customers a disservice.

BREAKING THE SOUNDBITE BARRIER

Hopefully no-one in this industry is telling customers that anti-virus is the only security application they need. Corporations and consumers take a big risk when they rely entirely on technical (part-)solutions to protect them, rather than learning enough about the issues to help themselves. Irritatingly, many AV-bashing articles of the type discussed here have skipped this point: they're not about solving the problem so much as replacing 'signature anti-virus' with their own products. Ironically, there seems to have been a shift in the last year or two towards the AV researcher view that even Kevin Townsend acknowledges:

> 'Well, if you ask an AV researcher he or she will always tell you, "I never suggest that AV is all you need – it should be part of a layered defence".'

What I'm not seeing from marketers inside and beyond the anti-malware industry is recognition that customers need to be educated enough to break the soundbite barrier and see through the hype. If we just tell customers that we're serving TOAST, we may be condemning *them* to being toast.

REFERENCES

[1] Intrusion Detection FAQ: What was the Melissa virus and what can we learn from it? SANS. http://www.sans.org/security-resources/idfaq/what_melissa_teaches_us.php.

[2] Hawes, J. Respecting the testing. Virus Bulletin. https://www.virusbtn.com/virusbulletin/archive/2006/09/vb200609-comment.

[3] Harley, D. AV Testing SANS virus creation. Virus Bulletin. https://www.virusbtn.com/virusbulletin/archive/2006/10/vb200610-sans.

[4] Consumer Reports Creates 5,500 Viruses For Tests (16 August 2006). SANS. http://www.sans.org/newsletters/newsbites/viii/65#320.

[5] Dunn, J. E. Antivirus software a waste of money for businesses, report suggests. Tech World. http://www.techworld.com/news/security/antivirus-software-waste-of-money-for-businesses-report-suggests-3412999/.

[6] Harley, D. Imperva, VirusTotal, and whether AV is useful. WeLiveSecurity. http://www.welivesecurity.com/2013/01/03/imperva-virustotal-and-whether-av-is-useful/.

[7] Harley, D. Signatures newsflash: AV doesn't detect what it doesn't detect. IT Security. http://itsecurity.co.uk/2015/07/signatures-newsflash-av-doesnt-detect-what-it-doesnt-detect/.

[8] Ion, I.; Reeder, R.; Consolvo, S. "...no one can hack my mind": Comparing Expert and Non-Expert Security Practices. https://www.usenix.org/system/files/conference/soups2015/soups15-paper-ion.pdf.

[9] Pauli, D. Choc Factory research shows users just don't get security. The Register. http://www.theregister.co.uk/2015/07/24/noone_can_hack_my_mind_google_experts_paper/.

[10] Hall, K. NHS XP patch scratch leaves patient records wide open to HACKERS. The Register. http://www.theregister.co.uk/2014/11/10/thousands_of_patient_records_at_risk_from_hackers/.

[11] Harley, D. Anti-virus Lives to Fight Another Day. Infosecurity magazine. http://www.infosecurity-magazine.com/opinions/anti-virus-lives-to-fight-another-day/.

[12] Smith, R. W. Anti-Virus: Little More Than a Team Player. Infosecurity magazine. http://www.infosecurity-magazine.com/opinions/anti-virus-little-more-than-a-team/.

[13] Harley, D.; Bridwell, L. Death of a Salesforce: whatever happened to anti-virus? https://geekpeninsula.files.wordpress.com/2013/11/death-of-a-salesforce-paper-final.pdf.

[14] Harley, D. Anti-virus: last rites, or rites of passage? Virus Bulletin. https://antimalwaretesting.files.wordpress.com/2013/05/dharley-feb2013.pdf.

[15] Journalism's Dirty Little Secret. https://antimalwaretesting.wordpress.com/2013/01/02/journalisms-dirty-little-secret/.

[16] (IN)SECURE, Issue 46. http://www.net-security.org/dl/insecure/INSECURE-Mag-46.pdf.

[17] Castelnuovo, R. Outmaneuvered at Their Own Game, Antivirus Makers Stuggle to Adapt. New York Times. http://www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?_r=1.

[18] Townsend, K. The anti-virus industry does itself no favours. IT Security. http://itsecurity.co.uk/2015/07/the-anti-virus-industry-does-itself-no-favours/.

[19] Johnston, C.; Harley, D. Please Police Me. http://www.welivesecurity.com/media_files/white-papers/Please_Police_Me.pdf.

[20] AMTSO Fundamental Principles of Testing. http://www.amtso.org/download/amtso-fundamental-principles-of-testing/.

[21] Harley, D. Blaming the Victim… WeLiveSecurity. http://www.welivesecurity.com/2011/07/08/blaming-the-victim/.

[22] Harley, D.; Lee, A. Call of the wildlist: last orders for WildCore-based testing? http://www.welivesecurity.com/media_files/white-papers/Harley-Lee-VB2010.pdf.

[23] VB100 comparative testing. Virus Bulletin. https://www.virusbtn.com/vb100/index.

[24] Harley, D. I Have a Little (Wild)List*. WeLiveSecurity. http://www.welivesecurity.com/2010/02/16/i-have-a-little-wildlist-2/.

[25] Zwienenberg, R.; Ford, R.; Wegele, T. The Real Time Threat List. Virus Bulletin. https://www.virusbtn.com/conference/vb2013/abstracts/Zwienenberg.xml.

[26] Harley, D. I'm OK, you're not OK. Virus Bulletin. https://www.virusbtn.com/virusbulletin/archive/2006/11/vb200611-OK.

Editor: Martijn Grooten
Chief of Operations: John Hawes
Security Test Engineers: Scott James, Tony Oliveira, Adrian Luca
Sales Executive: Allison Sketchley
Editorial Assistant: Helen Martin
Developer: Lian Sebe
Consultant Technical Editor: Dr Morton Swimmer

Tel: +44 (0)1235 555139. Fax: +44 (0)1865 543153
Email: editorial@virusbtn.com
Web: http://www.virusbtn.com/