

2 Witches, Warlocks, and Wassenaar; or, On the Internet, no one knows you are a witch.

Gather round, neighbors!

Neighbors, I said, but perhaps I should have called you fellow witches, warlocks, arms dealers, and other purveyors of heretic computation. For our pursuits have been weighed, measured, and found wanting for whatever it is these days that still allows people of skill to pursue that skill without mandatory oversight. Now our carefree days of bewitching our neighbors' cattle and dairy products are drawing to a close; our very conversation is a weapon and must, for our own good, be exercised under the responsible control of our moral betters.

And what is our witchcraft, the skill so dire that these said betters have girt themselves to "*regulate your shady industry out of existence*"? Why, it's apparently our mystical and ominous ability to write programs that create "*modification of the standard execution path of a program or process in order to*

allow the execution of externally provided instructions". We speak secret and terrible words, and these make our neighbors' softwares suddenly and unexpectedly lose their virtue. The evil we conjure congeals out of the thin air; never mind the neglect and the feeble excuses that whatever causes the plague will not be burned with the witch.

Come to think of it, rarely a suspected witch or a warlock have had the case against them laid out in such a crisp definition. Indeed, the days of *spectral evidence* are over and done; now the accused can be confronted with an execution trace! The judgment may pass you over if you claim the sanctuary of your craft being limited to Hypervisors, Debuggers, Reverse Engineering Tools, or—surprise, surprise!—DRM; for these are what a good wizard is allowed to exercise. However, dare to deviate into "*proprietary research on the vulnerabilities and exploitation*



of computers and network-capable devices”, and your goose is cooked, and so are your “*items that have or support rootkit or zero-day exploit capabilities.*”¹

Heretics as we are, we turn our baleful and envious eye towards the hallowed halls of science. Behold, here are a people under a curious spell: they *must* talk of things that are not yet known to their multitudes—that which we call “zero-day”—or they will not be listened to by their peers. Indeed, what we call “zero-day” they call a “discovery,” or simply a “publication.” It’s weird how advancement among them is meant to be predicated on the number of these “zero-day” results they can discover and publish; and they are free to pursue this discovery for either public and private ends after a few distinguished “zero-days” are published and noted.

What a happy, idyllic picture! It might or might not have been helped by the fact that those sovereigns who went after the weird people in robes tended to be surprised by other sovereigns who had the fancy to leave them alone and to occasionally listen to their babbling. But, neighbors, this lesson took centuries, and anyway, do we have any goddamn robes? No, we only have those stupid balaklavas we put on when we sit down to our kind of computing, and that doesn’t really count.

Ah, but can’t we adopt robes too, or at least just publish everything we do right away², to seek the protection of the “publish or perish” magic that has been working so well for the people who use the same computers we do but pay to present their papers at their conferences? Well, so long as we are able to ditch our proprietary tools and switch to those that mysteriously stop compiling after their leading author has graduated—and what could go wrong? After all, it’s mere engineering detail that the private startups and independent researchers ever provide to a scientific discipline, and they could surely do it on graduate student salaries instead!

But, a reasonable voice would remind us, not all

is lost. Our basic witchcraft is safe, for the devilish “*intrusion software*”, our literal spells and covenants with the Devil, is not in fact to be controlled! We are free to exchange those so long as we mean to do good works with them and eventually share them with our betters or the public. It’s only the means of “generating” the new spells that must be watched; it’s only methods to “develop” the new knowledge that you will get in trouble for. Indeed, our precious weird programs are safe, it’s only *the programs to write these programs* that will put you under the witches’ hammer of scrutiny. We have been saved, neighbors—or have we?

I don’t know, neighbors. Among the patron saints of our craft we distinguish the one who invented programs that write programs, and, incidentally, filed the first bug (if somewhat squashed in the process), and the one whose Turing award speech was about exploiting such programs—so important and invisible in our trust they have become, so fast. We spend hours to automate tasks that would take minutes; we grow by making what was an arcane art of the few accessible to many, through tools that make the unseen observable and then transparent.

Of all the tool-making species, we might be the most devoted to our tools, tolerating no obscurity and abhorring impenetrable abstraction layers left so “for our own benefit.” And yet it is this toolmaking spirit that we must surrender to scrutiny and a regime of prior permission—or else.

Is it merely a coincidence that the inventor of the compiler is also credited with “It is much easier to apologize than it is to get permission”? Apparently, there were the times when this method worked; we’ll have to see if it sways the would-be inquisitors into our craft of heretical computations.

Thank you kindly,
—PML

¹<https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items>

²Affording the time for proper peer review, of course, that is, the time for the random selection of peers to catch up with what one is doing. But what’s a year or two on the grand Internet scale of things, eh?