

OPINION

LEARNING FROM SONY: AN EXTERNAL PERSPECTIVE

Dan Kaminsky

DoxPara Research, USA

‘What happens when the creators of malware collude with the very companies we hire to protect us from that malware?’ Bruce Schneier, one of the godfathers of computer security, was pretty blunt when he aired his views on the AV industry’s disappointing response to the *Sony* rootkit (for an overview of the rootkit and its discovery see *VB*, December 2005, p.11). His question was never answered, which is fine, but his concerns were not addressed either, and that’s a problem.

The incident represents much more than a black eye on the AV industry, which not only failed to manage *Sony*’s rootkit, but failed intentionally. The AV industry is faced with a choice. It has long been accused of being an unproductive use of system resources with an insufficient security return on investment. It can finally shed this reputation, or it can wait for the rest of the security industry to finish what *Sony* started. Is AV useful? The *Sony* incident is a distressingly strong sign that it is not.

All things being equal, I’d rather have the AV industry on our side. We take it for granted that there are customers for private computer security services. It didn’t have to be this way: someone had to convince users that they were responsible for their own security. Because of the pioneering work of the AV industry, effective cryptography was non-negotiable, security research could be legitimate, and a free market for security technologies could form. Indeed, even the spread of broadband and WiFi would have failed if users hadn’t been motivated to purchase firewalls to protect their new high-speed networks. The AV industry made sure the users knew they needed to protect themselves, which is why it is such a great problem when the AV industry refuses to protect them.

TAKING CONTROL

Let’s be honest; the AV industry is blessed. What other software producers can depend on the operating system (for home users) or corporate IT departments (for the office) essentially demanding that their product runs on every system? When was the last time you saw a machine banned from a network for not running *Photoshop*?

What is it that customers think they’re purchasing when they buy anti-virus software? Is it just safety? The safest machine is the one that is turned off. In fact, users are looking for something beyond mere safety. Users want control – and they’re willing to pay for it.

We are in the business of putting force behind consent. Put simply, why ask for something if you can just take it? And let's make no mistake, *Sony* took control of people's systems. Whatever consent people may have granted initially to give *Sony* access to a system, it cannot be denied that *Sony* provided no mechanism for users to revoke that consent.

I often invite people into my home. I expect them to leave at some point, particularly if I ask them to. I certainly do not expect them to hide in my closet and pretend that they have gone. And if I call the police because the visitors won't leave, I don't expect them to argue with me about precisely what I agreed to when I first let them in.

Sony had a choice. DRM is unpopular software, as its primary purpose is to override user intent. *Sony* knew that some portion of users would want this stuff removed from their systems. They had the option to accept the revoked consent, and provide an uninstaller. Alternatively, they could simply ignore the need for user consent, take control of the system permanently, and simply prevent users from knowing there was anything to uninstall, by deploying a rootkit.

That the rootkit was exploitable by black hat hackers was bad, but ancillary to the argument. When the way you deal with users wanting to remove your code is by preventing users from *knowing* your code is running, not only are you operating without consent, but you know it, and everyone can tell.

BEEN THERE

Do we really expect the anti-virus industry to square up against companies when they are just trying to defend their copyright? Yes, absolutely. It's where the AV industry started.

We have just acknowledged the 20-year anniversary of the first PC virus, and almost everyone has missed the most interesting thing about it. *Brain* was not written by some random hacker, nor was it the nefarious creation of shadowy criminal groups. *Brain* was all too happy to identify its source:

```
Welcome to the Dungeon (c) 1986 Basit * Amjad (pvt)
Ltd. BRAIN COMPUTER SERVICES 730 NIZAM BLOCK ALLAMA
IQBAL TOWN LAHORE-PAKISTAN PHONE:
430791,443248,280530. Beware of this VIRUS...
Contact us for vaccination...
```

The first virus was written by an incorporated company. And why? *Brain* is still in business, so we can ask them. The following explanation can be found on the company's website (<http://www.brain.net.pk/aboutus.htm>):

'What no American journal had the courage to admit at that time was how badly the virus had hurt America's

painfully cultivated image of the world's leading copyright protector. Almost overnight, it had shown Americans to be the world's biggest copyright violators. Every time the virus found a new home in the USA, it signalled one more copyright violation by an American.'

Malware in the pursuit of copy protection is nothing new; the first PC virus was an unambiguous and unapologetic attempt to protect copyrights, by any means necessary.

It has been 20 years. It is time to recognize the threat of corporate malware. It is not as if corporate malware is a concept with which anyone is unfamiliar. One of the most glaring failures of the computer security industry in recent years has been the failure to prevent the spread of spyware. It took years for the anti-virus industry to start responding to spyware. The first anti-spyware code was released in 2000. One major vendor released nothing until 2003. Millions of systems were infected while nothing was done.

Eventually, the AV industry adapted. I attended a wonderful talk, not long before the *Sony* story broke, where I heard about the extraordinary steps the anti-virus industry was taking to deal with what can basically be summarized as 'hackers with lawyers'. As awful as it is that we have to deal with peer businesses, instead of kids and criminals, it certainly seems that the industry has finally learned to respond to these threats.

DEAFENING SILENCE

But there really was no response to the *Sony* situation. *Sony* claimed a few AV companies as allies, in order to give its actions the patina of legitimacy. That didn't work. The idea of *Sony* and AV companies in talks was received about as well as if the AV companies had been negotiating with the author of *Slammer*, agreeing on which exploit he was allowed to hit next.

A few AV companies added code to their products to remove the cloaking component of the rootkit, but as far as I know, nobody actually removed the DRM components for which users were so clearly trying to retract consent. Only banal excuses, such as 'we're waiting for *Sony* to write an emergency uninstaller', were heard.

Do we wait for the authors of worms to release uninstallers to clean up their mess? Even if they did release one, should we trust people who have written malware in the past?

Given that *Sony's* first uninstaller consisted of a patch to the latest version, and given that *Sony's* code already had a history of unintended security side effects, it was not a surprise to witness multiple useless uninstallers coming out of *Sony* over the next six weeks. (And this was after *Sony*

had decided to behave and respond in an extraordinarily responsible manner!)

There is one industry that knows how to write an emergency uninstaller, one that's safe, effective and that can be released quickly. But the AV industry did nothing.

Some have claimed that it would actually have been illegal to have interfered with the *Sony* DRM, due to the Digital Millennium Copyright Act (DMCA). These claims have some merit – the US's DMCA does indeed take a rather dim view of subverting copyright protection mechanisms. Ignoring the fact that not all AV companies are American, and that not all victims were American, this legal interpretation opens up an astonishing attack vector.

Imagine a startup – we'll call it *MP3Solutions*. *MP3Solutions* would combine spyware with DRM. First, they'd design some code that detected watermarks in MP3 audio. Then, they'd offer \$10 per deployment to independent third parties, 'no questions asked'. The code could be spread via worms, botnets, or drive-by web installs, but since the payload was copy protection software, the DMCA-fearing AV industry would just have to sit back and fail to protect anyone.

It really is amazing what happens once a user's consent to operate is considered optional. If this is really how the AV industry is interpreting the DMCA, that's astonishing and newsworthy. But the DMCA restrictions certainly would not have prevented the AV industry from complaining, or even asking for explicit permission to remove this particular piece of malware. Such permission seemed likely to be granted in this case: by the end of November, *Sony* was taking aggressive steps to manage the situation responsibly, providing free MP3s to affected customers and displaying a banner ad to inform users of their situation. The only thing *Sony* was having trouble with was an effective uninstaller – certainly they could have used the assistance of the AV industry!

Perhaps such a request was made, and permission was not forthcoming. It's possible. But another thing the DMCA does not do, is ban the provision of a warning to customers that the service they've purchased would be illegal in this instance: 'Software has been detected on your system whose operation you may not consent to, but which we are legally forbidden to remove. The vendor refuses to provide consent for us to remove this software for you. Please contact the following vendor address [link] to ask why.'

But instead, *Sony* got the benefit of the doubt.

We don't pay the AV industry to give *Sony* the benefit of the doubt. The AV industry cannot take money from users and provide services to *Sony*. I call upon every anti-virus company to state publicly that, the next time a media

company tries to take control of users' PCs, and decides that the continued consent of the computer owner isn't necessary, they will act.

IN CONCLUSION

The AV industry in general failed to handle the *Sony* situation responsibly. I am confident that such a widespread failure will not be repeated – which means that those in the AV industry who do stand up and act will be well placed to take business from those in the industry who do not. By all accounts, the failure to respond to *Sony* was a business decision. *Sony* is a massive organization, one that possibly represents a significant opportunity. Why anger the giant?

You don't have to stand up for users. But your customers don't need to pay you. I spent many years working through security policies. Many demanded anti-virus software on every system. Not one of them cared about the size of the organisation that wanted the malicious code installed.

However big *Sony* is, the AV industry left even larger customers out to dry. (Military sites were hit. Does the military operate without anti-virus?) AV sales people should expect to be asked a simple question: why should anyone pay you to protect someone else?

I call upon every anti-virus vendor to state, solemnly and verifiably, that what happened with *Sony* was an anomaly – a misunderstanding based on an incomplete understanding of what customers demanded. No AV company expected this reaction. Certainly, *Sony* had no idea of the firestorm they were walking into. Did they ask? What were they told? Regardless, with this new data can come new policy.

I also call upon the AV industry to stop releasing bad data. I do apologise for implying publicly that AV companies knew precisely how many *Sony*-infected nodes were out there. You can't manage what you can't measure, and thus I had assumed that AV companies were measuring what they were trying to manage. I know now that some of them just look at how many tech support calls they get, and extrapolate.

That is awful. The plural of 'anecdote' is not 'data'. Expect any further releases of numbers to have their methodology questioned. As for my own data – those who are curious about my own methodology for tracking the *Sony* rootkit are welcome to look through the 85 gigabytes of anonymised compressed DNS traffic that I used to build my estimates (see <http://www.doxpara.com/?q=sony>). One researcher with a high-speed net connection should not have better data on a global scale malware attack than companies with customers paying them to manage that malware. And yet, I have almost a tenth of a terabyte, and they have tech support calls.

I invite the AV industry to do better.