Malware infecting hard disk firmware remained hidden for 15 years – but who's responsible?

February 20 2015, by Alan Woodward

Picking off hard drive manufacturers, one by one. Credit: Kaspersky Lab

It sometimes seems that whenever security researchers discover some new exploit or malware that allows the monitoring of remote computers, the finger is quickly pointed at the US intelligence agencies.

Security firm Kaspersky has recently revealed a complex malware developed by a group called Equation. Although its report made no mention of the US National Security Agency, subsequent news reports held it responsible anyway.

This seems to follow the logic that, as Equation's malware uses techniques similar to Stuxnet, if Stuxnet was developed by the NSA then Equation's must also have been developed by the NSA. But despite everything that's been written about Stuxnet's origins, there's no conclusive proof tying it to the NSA, or anyone else.

Such breathless headlines unfortunately obscure how interesting this new suite of malware is – not least that it isn't new, but dates back to 2001. That is eons in technological terms.

Hard drive attack

What's also interesting is the way the attackers hid the malware: by embedding the malicious code into the firmware (hard-coded software) built into hard disk drives found in practically every computer. Not just drives from one manufacturer, but almost all the mainstream brands – perhaps even the one that powers the computer on which you read this now. Why is this important? It means you could wipe the entire drive, reinstall your computer's software from scratch – and still be infected.

The only more attractive hiding place for an attacker is the firmware that is required to start the computer, the BIOS, but viruses that attack the BIOS have been around for decades and hardware has been adapted in defence. On the other hand, looking at hard drive firmware and adopting defences against tampering with it just hasn't been on the agenda, a fact that has allowed this malware to go undetected for so long.

An updated, evolving threat

And it's not just that the attackers were able to work out how to embed their malware in the drives' firmware; they appear also to have been able to update it with improved versions. This would require updating

("flashing") not just the malware but the original firmware code too, without which the drive wouldn't function. This is considered technically advanced even today – yet someone seems to have developed the capability to do so more than 10 years ago. This is technically impressive.

So the fact that such an advanced technique was deployed so long ago prompts us to wonder what else is out there that we don't know about? It's not as if this is the first such discovery: Stuxnet, Flame, Regin and now Equation, all of which appear to have been active for many years. To paraphrase Oscar Wilde: to miss one piece of malware looks like misfortune, to miss four looks like trend.

Pointing the finger

It is easy, as we see from some of the headlines, to attribute blame based upon circumstantial evidence such as those who was attacked. However, this assumes that a state actor is responsible – and that only certain countries have the wherewithal to develop such a capability. Yet, as the video above demonstrates, one individual with skills and time was able to do much the same.

One of the extraordinary things about cyber warfare and cyber espionage is how it has levelled the playing field between adversaries who might be hugely unequal in other ways. With a relatively small team and modest budget anyone could potentially develop very clever software. Cyberspace is the ideal platform to wage asymmetric warfare.

The reports of all these threats – Regin, Stuxnet, Flame, and others – carry the assumption that a government is responsible. It's not an unreasonable assumption considering that the software's primary function is espionage. But while nation states are the consumers of intelligence gathered in this way, it doesn't mean that their agencies are

responsible – there is an active market for such information, which means there is a commercial motivation for others to collect it.

Criminal hackers steal personal information to sell on the black market to those who would commit fraud. They might equally gather data of interest to governments and law enforcement and sell it to them. In many ways it is a classic market: with limitless demand there will always be those willing to supply.

In any event, it's worth reading the full range of reports available and forming your own judgement. Like reading only a single newspaper, the likelihood is that the news is reported with a particular slant – such as blaming the NSA. And while you can be sure of very little when it comes to final attribution of these attacks, you can be sure that individual reports carry their own bias. If you are able, it is worth concentrating on the technical detail as that is where you're more likely to find the truth.

And expect to hear more such stories in the future – after all, if malware can be hidden so succesfully 10 years ago imagine what's possible today.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation