

Anti-virus: a technology update

Anti-virus software might be the archetypal security product, but with so many high-profile malware attacks – including Stuxnet and Zeus – is it doing its job? **Kevin Townsend** investigates whether anti-virus software is still relevant

Anti-virus was the first, the most ubiquitous, and is certainly the best known defence against the bad guys. Hugely damaging successful malware attacks, however, beg the question: Are the bad guys winning the arms race?

“The key thing to recognise”, says James Lyne, senior technologist at Sophos, “is that these things are now so inextricably linked that this aged distinction between things like viruses, worms, trojans and spam actually doesn’t make a lot of sense at all – it’s all just ‘bad stuff’”.

Bots on compromised PCs, for example, are used to deliver spam that contains social engineering scams designed to trick users into visiting malicious websites. This website will then infect the user with a trojan that opens a back door to allow in a root kit containing a keylogger and spyware. Anti-virus software doesn’t just seek to protect you from viruses, then, it seeks to protect you from all of this bad stuff. For the sake of this article, we’ll just call it all ‘malware’.

What are the attackers doing?

Modern malware has evolved from a demonstration of personal prowess into a serious, organised criminal business, driven by the same motive as any legitimate business – a desire to maximise return on investment (ROI).

Wherever there is a large concentration of users, there will also be malware. This explains the malware campaigns on Facebook and Twitter. But it also tells us what is likely to happen next – increasing malware for the Mac (a new Mac version of KoobFace was discovered by Intego, a Mac security specialist, at the time of writing).

Criminals follow the people, and as the Mac and other Apple products increase in popularity, so do the criminals who attack them.



Thanks to the cloud, [reputation] is instantly available to all of our other customers

Rik Ferguson

Mobilisation is one of the biggest computing movements today. As mobile computing and smart phone markets grow, they attract malware. Similarly, market growth in virtual machines will lead to attacks on

the hypervisor. The AV industry is aware that there are proof-of-concept attacks on virtual machines, but nothing has yet been found in the wild. It will eventually happen; and anti-virus companies are waiting.

It is only with a degree of tongue in cheek that Luis Corrons, technical director of PandaLabs, introduces the idea of anti-virus for fridges. “Everything is connected to everything else, and it’s all connected to the internet”, he says. “I don’t know that we’re going to install anti-virus for the fridge, but who knows.” If there are enough fridges connected to the internet, fridge malware will no doubt follow suit.

Technical sophistication

Lyne describes one example of the increasing sophistication in malware. “Polymorphism”, he says, “has been around for about 20 years. It’s where the malware continually changes itself to avoid detection – but it has been easy for the AV vendors to defeat it. But today, the bad guys are using server side polymorphism where the engine is not in the malware but on legitimate business websites. Every time it is refreshed, what is downloaded is different in content to the previous download, and after a couple of hundred downloads, they kill that site and move on to another. That way, none of us vendors

DEVELOPMENTS IN CONSUMER ANTI-VIRUS

The biggest single development in consumer anti-virus offerings is the growth of the free product. Many companies now provide free online scanners – Trend Micro's HouseCall and Symantec's Security Check are good examples. There are also a growing number of free products you can download and install on your computer: AVG and Avira are well-known. More recently, Panda has launched a new free version.

Petter Lautin, Panda Security's MD for UK and Ireland, explains the rationale: "A Morgan Stanley survey in America has shown that 46% of consumers rely on free security software, and that's expected to increase to nearer 60%. I'd be surprised if things in Europe are very different; so that's a fact of life we can't ignore. Secondly, believe it or not, there are many people out there who are still not using any anti-virus product at all. For them, this is a perfect way to start because it gives you the basic anti-malware protection that everyone needs to have. From there we can start to talk about what you should have rather than must have: a firewall, ID theft protection and all sorts of things on top of that."

ESET's David Harley has a pragmatic view. "The economics of the marketplace, though, are that the consumer market isn't really profitable. It costs more than some companies can afford to support those customers, measured against the profit margin. That's why some companies make single-user licences so expensive compared to their corporate deals. So for years, the deal with free AV has been a trade-off: fewer bells and whistles and often less detection/disinfection, and restricted support (forums, but not telephone support)."

There is still a dearth of AV software for the Mac. "There is a limited number of anti-virus tools for Mac", explains Laurent Marteau, CEO of Intego, one of the relatively few Mac AV vendors. "With Mac anti-virus software, none of the companies offering free tools have the infrastructure to find Mac malware and update their software in a timely manner."

This is about to change, however, as Sophos released the industry's first free AV package for the Mac as this issue goes to press. Watch this space.

can get hold of the engine to write any form of generic protection."

Unfortunately, there doesn't appear to be a major advance in AV technology on the near horizon. "Right now", says David Harley, ESET research fellow and director of malware intelligence, "it's more a case of multiple/hybrid technologies (found in nearly any modern AV) advancing by improving individual components. Obviously, some products stress certain components more than others."

Christopher Boyd, GFI senior threat researcher, suggests "virtual sandboxing, which allows threats to be intercepted and executed inside a virtual machine running a Windows-like pseudo environment, allowing for more accurate detection and safer quarantine and disposal".

Your reputation precedes you

Possibly the biggest single development in the AV world has been the evolution of product-based reputation feedback (not to be confused with community-based reputation systems such as the web of trust). Rik Ferguson, Trend Micro's senior security advisor, explains his own company's reputation system, born out of the marriage in the cloud of three separate databases: bad emails, bad URLs and bad files.

"Let's take a hypothetical worst-case scenario", he says. "You get an email from a bot that has only just been infected, and the email is well-crafted so it looks OK. We can't see anything wrong with it, so we allow it. In this case, email reputation has failed. The email contains a link to a malicious website that has only just been registered. We don't yet know that it's bad so we allow

you to click the link, and again the reputation system has failed", he explains. "You click the link and visit the website which uses a zero-day exploit to infect you with a new trojan that the bad guys have already tested against all the AV products. We haven't seen this trojan, so we allow you to download it and you become infected. Email, URL and file reputation systems have all failed."

But, he stresses, continuing on to a happy ending, "the first thing that the trojan will seek to do is phone home, either to tell its owner that it has landed,



So for years, the deal with free AV has been a trade-off: fewer bells and whistles and often less detection/disinfection, and restricted support

David Harley

or to download additional components. At this point we will almost certainly recognise this as suspicious behaviour and block it. We will also relay the URL source of the suspect file to TrendLabs who will download the page content and analyse it." Instantly, the URL database and file database are updated with the new



Are Stuxnet and Zeus proof that anti-virus software is not protecting your computer well enough?

