Is the time for antivirus software past?

Warwick Ashford Thursday 27 June 2013 12:06

Since the first appearance of malware in the 1970s, business adoption of antivirus (AV) software has grown steadily and become fairly well established, but is it time to move on?

AV suppliers will argue – and many information security professionals agree – that AV software still has a place, but they all say that the time has come for a more proactive approach to security. Evidence that things have changed radically in the past few years can be found in the number of unique types of malware being detected on a daily basis.

According to security firm Kaspersky Lab, the rate of detection jumped from one new type of malware appearing every minute in 1994, to one every second in 2012, to one every half second in 2013. This translates into 200,000 unique new malware samples being produced on an industrial scale every day, which is practically impossible for any signature-based AV software system to cope with.

This step change is similar to the step change that faced code-breakers in the Second World War, when the introduction of machine-generated codes outstripped the capabilities of First World War analysts.

AV software still has a place, but the time has come for a more proactive approach to security

Classicists and linguists were no longer able to crack the codes produced by the infamous Enigma machine, ironically patented in London in 1925, and later adapted for military use by Nazi Germany. It was only through the work of mathematicians such as Dilly Knox, Alan Turing, Gordon Welchman and others at GCHQ forerunner Bletchley Park that the Enigma machine codes were broken. Similarly, while AV is still necessary to take care of well-known attacks – and Kaspersky Lab has a database of 100 million of those – that alone is no longer enough to provide data security.

Moving beyond AV software as cyber threat evolves

As cyber criminals switch their attentions predominantly to business in pursuit of financial rewards, the mass production of sophisticated threats is being driven by the advent of crimeware kits in 2010. This means a greater number of people are able to make money from cyber crime without having to have a high level of technical expertise, said Bob Burls, director of Centaurine Consulting. “This gave rise to ‘point and click’ criminal activity, in which cyber criminals can easily buy or rent all they need to carry out attacks,” he said.

According to David Emm, senior regional researcher for Kaspersky Lab UK, this evolution in cyber criminal activity means that the bulk of the security firm’s malware detection no longer relies on signatures.

Instead, the threat landscape demands a combination of security technologies, including heuristics, sandboxing, emulation, whitelisting, and real-time analysis and updates using a cloud infrastructure.

User's present an entry point for attackers

Despite the challenges, securing computers remains easier than securing users, said Emm, observing that most high-profile breaches involve social engineering to manipulate users to do risky things.

The classic example is of RSA employees who opened infected emails with juicy subject lines even though the emails had been trapped by the company’s spam filter.

Although infected emails are still one of the most common ways of getting malware aimed at establish an entry point for attackers, distribution techniques are also getting increasingly sophisticated. Compromised legitimate websites have fast become the top way for infecting computers through drive-by downloads, which are invisible to the user. Social networking sites are also providing a rich source of data collection by cyber criminals as many people tend to “over share” valuable personal information.

“Information about a recent business trip, for example, can be used to make a spear-phishing email more plausible by referencing the trip’s destination and purpose,” said Emm. Security firms are turning to the cloud to enable proactive defences to provide near real-time responses

This type of information gathering is synonymous with targeted attacks, which now make up around 10% of all attacks, but researchers to expect this to continue to increase, he said.

Because of the increasing interconnectedness of organisations, everyone is now in the frame for targeted attacks, said Vincente Diaz, senior malware analyst at Kaspersky Lab.

Again, the classic example is that RSA was breached, but its customer, Lockheed Martin, is thought to have been the ultimate target.

Considering the scale and sophistication of attack and distribution methods, and the fact that new technologies such as virtualisation, cloud and mobile are attracting attackers, the days of AV-only are over. In the light of the fact that attacks are evolving at internet speed, security firms such as Kaspersky Lab are turning to the cloud to enable proactive defense to provide near real-time responses.