



Trend Micro: Antivirus industry lied for 20 years

30 Jun 2008 11:10

Chief executive Eva Chen argues antivirus companies have over-hyped the effectiveness of their products, and misled customers, for years

Eva Chen, chief executive of Trend Micro, has strong views about how effective the antivirus industry has been over the past 20 years.

According to Chen, the security industry has over-hyped how effective its products are — and so has been misleading customers — for years.

Chen believes that no single company can offer adequate protection against the sheer volume of new viruses that are being churned out by cybercriminals. According to the security industry, five and a half million new samples were detected in 2007.

Q: Trend Micro has recently [moved to an 'in-the-cloud' service](#). Surely traditional security methods are still effective enough?

A: In the antivirus business, we have been lying to customers for 20 years. People thought that virus protection protected them, but we can never block all viruses. Antivirus refresh used to be every 24 hours. People would usually get infected in that time and the industry would clean them up with a new pattern file.

In the last 20 years, we have been misrepresenting ourselves. No-one is able to detect five and a half million viruses. Nowadays there are no mass virus outbreaks; [malware] is targeted. But, if there are no virus samples submitted, there's no way to detect them.

But how about analysis using other methods? You don't need to rely solely on antivirus.

Every year there's a new industry buzzword, but they always fail. Heuristics use a rule to inspect the file, but virus writers know this. They split the complete malicious program into different files, and download each file to test it against the heuristic rule. Each file looks innocent but, when combined, they become a virus.

Three years ago, the buzzword was 'personal firewalls', but you can't block everything. To have an effective personal firewall, you'd have to block port 80, but HTTP uses port 80. If you blocked that, no-one could use [the internet].

HIPS [host-based intrusion-prevention systems] have a lot of rules to tell if this application is trying to touch another application. HIPS behavioural monitoring requires files to be executed, so virus writers make sure they evade the rules.

So isn't 'in-the-cloud' computing suffering from the same hype?

Trend Micro has gone to cloud computing because it's a necessity. Usually, hackers now <http://www.zdnet.co.uk/misc/print/0...>

17/09/2008

Trend Micro: Antivirus industry lied f...

Trend Micro has gone to cloud computing because it's a necessity. Usually, hackers now infiltrate websites. When a user clicks on a URL they are redirected to a malware-hosting site. They download the first components, usually a downloader, which downloads more components and a recomplier.

Two Trend Micro sites were [infiltrated in March](#), weren't they?

That shows that it's everybody's problem. Our websites were outsourced and, in [website code], there are a lot of commands that can be compromised. An attacker can insert an Iframe through SQL injection. It was an Iframe-injection attack on the page we outsourced to a developer. I don't know which development company it was.

Do you know who attacked the Trend Micro sites?

We don't know who did it. It was a mass attack — 20,000 sites — so very hard to trace.

Trend Micro is in the process of a [lawsuit against Barracuda Networks](#) over a patent dispute. As Barracuda uses the open-source ClamAV engine, there has been disquiet in the open-source community that any company that incorporates ClamAV into a gateway-security product will be sued by Trend Micro. Is this the case?

I'm suing Barracuda, not ClamAV. The patent is about how to stop viruses in transmission. We've traded patents with IBM and Symantec, and settled with McAfee when they were Network Associates. We won the litigation with Fortinet. We respect other people's intellectual property; we just want people to respect ours. This has nothing to do with free software. It's about the implementation.

[Story URL: http://resources.zdnet.co.uk/articles/features/0,1000002000,39440184,00.htm](http://resources.zdnet.co.uk/articles/features/0,1000002000,39440184,00.htm)

Copyright © 1995-2008 CNET Networks, Inc. All rights reserved

ZDNET is a registered service mark of CNET Networks, Inc. ZDNET Logo is a service mark of CNET Networks, Inc.