

> interview

RICHARD STIENNON
CHIEF MARKETING OFFICER, FORTINET INC.

“Windows Vista...will do nothing to slow down the growth of cyber crime”

Richard Stiennon is the chief marketing officer at Fortinet Inc and a network security industry expert with more than 25 years of experience. An acknowledged and acclaimed industry thought leader, he is perhaps best known for his tenure as vice president - Research for Gartner's security and privacy group, where he regularly provided strategic counsel to Global 2000 CIOs and earned Gartner's Thought Leadership Award for 2003. Here Stiennon shares his candid assessment of the cyber threatscape in 2007. According to him, attackers have now evolved into hatching 'business models' and 'gunning for the big boys' with business-focused strategies. He sees 2007 as the year in which cyber criminals wise up and go for a bigger slice of the pie. Excerpts:

How do you view the current trends in cyber crime across the world and what do you foresee in 2007?

Cyber crime is a healthy new industry that is growing at least 100% a year. The major growth comes from new participants and the development of markets for identities and the services around exploiting them.

I predict that the quest for financial gain will spur cyber criminals to a banner year, at least doubling their overall take. This will be an organic growth. In other words, it will not stem from some sort of brand new cyber attack but will come from the type of growth the Internet is famous for. The number of victims is growing with the Internet and the number of cyber criminals is growing even faster than that.

What actions do you think are required to be taken up to counter the threat?

The most effective actions would be better cooperation between law enforcement agencies around the world. There are some encouraging developments as the G8 countries are working toward better communication and prosecution.

How do you see the launch of Windows Vista as a measure to restrict data theft and network security?

Windows Vista, while incorporating better default settings and offering Microsoft AV, will do nothing to slow down the growth of cyber crime. For an individual it is a good measure of defense. But the impact on cyber crime will be minimal.

Further, the introduction is too late. Adding basic security to Windows is not enough to mitigate the rising tide of cyber crime. It may be several years before Vista represents more than 50% of all machines, but by then the attackers will have matured and refined their tools to the point where Microsoft cannot keep up.

What are the mitigation measures that security specialists can adopt in view of the impending threats?

They can re-architect their DNS infrastructure to be distributed and put it behind robust firewalls. They should do regular vulnerability assessments of all Internet facing assets such as web servers, databases, etc. Sensitive data



should always be encrypted when it is at rest (credit cards, etc.). They should use strong authentication for access to valuable services such as banking, health records, etc. Intrusion prevention capabilities need to be deployed at the edges of their network.

Just as attackers are adopting 'business models' in their approaches, how will the IT security industry counterpunch?

The industry has been very reactive. Not their fault because customers are very slow to invest in security technology. They wait until they have suffered measurable damage before reacting. The long-term change will be that security will infuse every part of the IT industry. It will not be an after thought. You will buy your network gear from a security vendor for instance, instead of buying your security gear from a network vendor.

Now that there is spread of wireless applications, what efforts are necessary to control its misuse?

The carriers and providers of cell phone networks and WiFi hotspots should filter viruses and spam "in the cloud". If your cell phone runs a vulnerable OS, you should consider using a mobile security client.

What are your plans to control data theft crisis in 2007?

Fortinet is working closely with major carriers, ISPs, and MSSPs to enhance their service offerings to include content filtering defenses in the cloud. We are also working with major retailers and e-commerce sites to defend their networks from cyber attacks.

— Vandita Agrawal