

Top 10 predictions for 2007

| BY RICHARD STIENNON |

As the drivers for cyber crime increase, there is a lack of inhibitors to counter the escalating threats. While escalating the use of technology, attackers are becoming more innovative in their development of lucrative business models. Now, more than ever, it is likely that these attackers — who were once satisfied with a paltry US\$100 here and US\$1,000 there — are gunning for the big boys. And in 2007, it is almost certain that they will pull out all the stops in trying to get it.

This could very well be the year that attackers get smart about attacking enterprise data caches in a fashion that could double their cyber crime revenue — moving their market to between US\$4 billion (about RM13.6 billion) and US\$8 billion. Cyber extortion attempts, however, will no longer be limited to financial institutions or enterprises, and even local governments, schools and manufacturers could find themselves trying to protect against normally business-focused attacks.

Here is my complete Top 10 Threat Prediction list for 2007:

- 100% growth in revenue for cyber crime: The cyber crime industry will increase its focus on enterprise data stores and drive up its profitability. Cyber crime industry revenue will come in between US\$4 billion and US\$6 billion next year, doubling the current overall take.
- DDoS in support of phishing attacks: A combined effort between the phishers and the distributed denial of service (DDoS) attackers, with a social engineering twist, could result in an attack against a bank or e-commerce site. Attackers might also expand their targets for these types of threats beyond the usual outlets, so universities, local government agencies, publishers and manufacturers should consider clamping down on security.
- Successful DDoS attacks against financial

services firms: Although DDoS attacks are already in progress, 2007 will be the year that attackers attempt more high-profile targets.

- Threat of the year — attacks against DNS: Whereas DNS servers are a part of the critical infrastructure of the Internet, they are also an easy attack target because DDoS DNS servers are exposed by their nature and, because they control

where a browser is pointed, they could become the primary target for attackers that want to take down a website.

- Identity theft continues to rise: Markets are developing, which could make it easier to monetise stolen identities, thus increasing the value of stolen IDs while decreasing the cost of “moving” them.

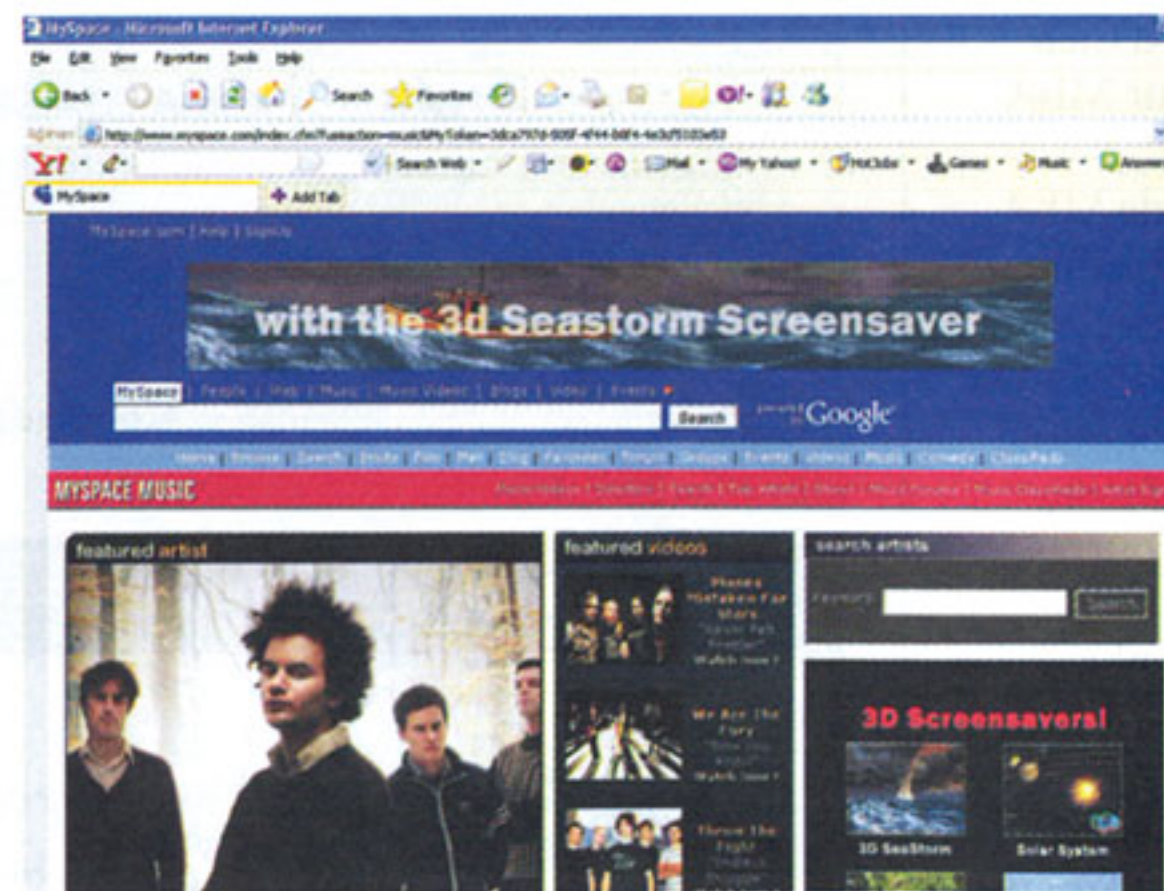
- More attacks against wireless networks: Attackers will continue their pursuit of victims through text messaging, “vishing” and malware that infects Symbian phones and spreads via Bluetooth or MMS.

• MySpace grows up and gets secure: In 2007, the number of attacks from predators, criminals and hackers will get to the point that MySpace will be forced to tighten its controls and monitoring. Unfortunately for MySpace, this will make it less appealing to its young adult audience.

- YouTube abuse: Like network news, email and IM before it, the new video-sharing trend will succumb to spammers who post ads, ad-backed videos and stealth-marketing exploits.

- Network infrastructure shows signs of overloading: The backbone providers have been resting on the excess bandwidth in which they invested during the dotcom bubble. Now that voice and video are really here, the infrastructure is showing signs of weakness. This could manifest itself in outages, slowdowns and a mad scramble to lay more fibre in 2007.

- Spread of Windows Vista will have zero impact on the overall threatscape: It may be several years before Vista represents more than 50% of all machines, and by then, attackers will have likely matured and refined their tools. Zero-day exploits for Vista are already available for purchase on the web. **E**



Among the predictions is that MySpace will be forced to tighten its controls and monitoring.

Richard Stiennon Fortinet is chief marketing officer of Fortinet