

Brace up for the threats ahead

It is not any one part of an organisation that would be affected by cyber crime this year. The entire IT infrastructure is vulnerable to attackers who are developing lucrative business models

RICHARD STIENNON

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

Cyber crime, a lucrative business

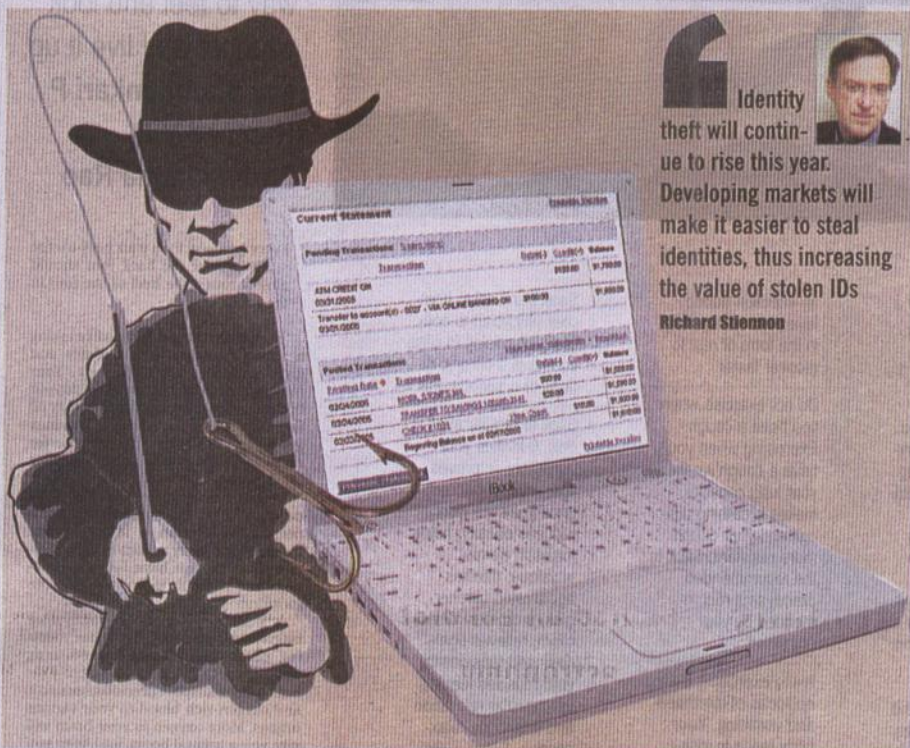
Cyber criminals are expanding their horizons. On the technology front they are researching and discovering zero day vulnerabilities in Windows (IFrames, WMF) and deploying them for profit. Cyber crime today has also become a very lucrative business, from the extortion attacks that garner tens of thousands of dollars to credit card theft which can earn the thief \$12 to 100 per stolen credit card. Cyber criminals are changing their MO to become much more entrepreneurial. They are learning to sell applications that make phishing attacks simple to launch. They manage the attacks from consoles. And they use a network of business partners to launder the money won from stolen IDs.

People today want to know about the part of organisations that would be affected the most. I would say that it is the entire IT infrastructure. The network only enables the hacker by providing the avenue of attack. Web applications are vulnerable to business process hacking, credit agencies, export-import and financial transaction sites have all been hit by attackers who purchase limited access and then abuse the underlying business logic to steal more information. Employees are vulnerable to social engineering attacks and bribery that could lead to stolen IP and personal data.

2007 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 \$4 billion and \$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.

Let's have a quick look at how threats are going to affect all of us in this year:

➤ **100 per cent growth in revenue for cyber crime:** The cyber crime industry will increase its focus on enterprise data stores and drive up its profitability. Stiennon's prediction is



Identity theft will continue to rise this year. Developing markets will make it easier to steal identities, thus increasing the value of stolen IDs
Richard Stiennon

that the cyber crime industry revenue will come in between \$4 billion and \$6 billion next year, doubling their 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 for 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 web site.

- **Identity theft continues to rise:** Markets are developing that 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 up 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 fiber 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 per cent 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. ■

The writer is Chief marketing Officer, Fortinet Inc.