

SPAM, SECURITY, AND SOCIETY

Sophos CEO Steve Munford was in Singapore toward the end of last year as part of his Asian tour. The nation is headquarters to most of its operations in the region, which is becoming increasingly important as China has gained prominence in recent times. *Computerworld Singapore* caught up with him to glean his insights into the latest industry developments as well as the most critical security issues facing CIOs today.

■ BY GERALD WEE

Computerworld Singapore: How have recent security threats been evolving?

Steve Munford: You've got a number of dynamics coming out. There are a lot of broader IT trends happening, that are causing issues for security: increased mobility, increased use of social media, increased use of Software as a Service applications, and lastly, just the whole proliferation of devices attaching to a computer. The increased threat is coming from the fact that there is a lot more opportunities to target machines as there is a lot of value in the data. This will lead to more creative threats.

What sort of trends do you see happening?

A couple of trends we are seeing. The whole spam problem which has been a problem for many years...we're seeing it becoming more prevalent and more sophisticated. This is because spam supports grey business. These are companies, for example, operating out of Russia selling counterfeit drugs under legitimate brand names like Viagra.

So, the company will have a website to sell you drugs which are manufactured in India as a generic, but they will market under a brand name.

The way spam comes into this is that they need people to go to their site, and they pay spammers to draw you to their site, and because there is so much profit to be made, they can afford to pay spammers a fair bit. We studied these sites, and the Website itself is making several hundred thousand dollars a day, therefore they are paying half of that to spammers. So, it is a distribution model like multilevel marketing.

I was giving a talk on this, and someone came up and said they actually bought drugs off the site. If you go a site called CanadianPharmacy.com, it looks legitimate. You put your credit card in, and the product ships in three or four days, and you get your drugs.

They don't steal your credit card information, and they send you a product that works, but it is marketed illegally.



What makes spam so serious?

About 97 per cent of spam comes from infected computers. If I'm a spammer, I use these as relays to send spam, and collect money from partners. That is a good business, and if you are a malware writer, and you can get a network of infected computers, you can make good money doing that.

This is a fresh perspective from the traditional fear-mongering and stealing of information.

There is also the economy of stealing information, but the interesting thing about that is that it is so targeted and specific. It happens in two ways. You have the targeted attacks where individuals are going after companies to get credit card information or something like that, and that is a very specific attack. The second way, and the way which most data gets lost, is people accidentally doing something bad, like leaving the laptop in the taxi. The taxi driver sells the laptop, and that person looked at my hard drive, and find interesting information there. There have been countless such examples in the UK

involving laptops, smartphones or something like that, which get sold in the black market.

The other example is people accidentally sending out information like customer or employee lists, and with e-mail lists, you can easily get the wrong name. From what we hear, companies will lose 5 to 10 per cent of their laptops every year, and imagine if you are a consulting company, or ad agency, or an accounting firm. Those laptops have pretty sensitive information on them. So, there are two ways: the targeted threat, and the accidental loss.

Which is a more serious problem?

The accidental one. That is a more widespread problem, but don't get me wrong. If you are a CIO, you are very concerned about people stealing intellectual property, and corporate espionage. One organisation I know in the west is concerned about their competitors, particularly from China, getting such information. The speed at which they copy is prolific.

Do you agree that there is no such thing as 100 per cent security?

It is layers of security, and five years ago, if you had antivirus and firewalls, you were pretty secure. And the reason why is because most data resided within the corporation. You control data within the organisation and limit access to Internet—static web pages or e-mail. Now, in a world where there so much mobility and different types of sites with complicated threats, how can you be secure with that.

So, there must be layers—policy layers, protection layers, and worst case scenarios.