



Why spam is the most lucrative game in town

GORDON SMITH hears how spammers are becoming more sophisticated and why this makes them harder to stop

A self-confessed movie buff, Scott Weiss (pictured) has a celluloid analogy to describe the current spam problem.

As general manager of IronPort, now part of Cisco, he has seen most malware tactics in action for himself — to a point where he probably occasionally feels like a Hollywood studio executive, bombarded with scripts and story ideas.

According to Weiss, many computer owners are unaware their machine has been compromised to spew out spam and is simply awaiting orders to do its controller's bidding.

"Like in *The Manchurian Candidate*, it lays dormant until it gets the phone call saying 'it's time to kill the president'. Then it's time to start sending this spam," he says. Large groups of these controlled PCs are called botnets. "Botnets are where most of the spam is coming from today," he adds.

And the problem is showing no signs of diminishing. International spam levels rose by 39pc alone during September, according to figures from SoftScan. It classified 93.51pc of all messages as unsolicited junk mail, with levels over 98pc on some days. Locally, the situation is a little better.

"We've found on a good day 50pc of the total email sent will be spam and on a bad day

it's as high as 86pc," says Derek O'Beirne, operations manager with Topsec Technology.

"Legislative and technical efforts, in a sense, are fighting against a rising tide. Spam levels are increasing, firstly because spam works. If you're looking at billions of spam emails being sent every day, you only need a hit rate of .0001pc to make money. The real cost of spam is borne by the recipient," O'Beirne points out.

So sophisticated have spamming operations become that Weiss considers it a mini-industry complete with its own value chain.

First is the person who writes the Trojan Horse program to turn a PC into a bot. Then there is the botnet owner. A third party, the spam creator, might simply rent 'time' on the botnet from its owner. There's enough money to be made that everyone can afford to specialise in each task.

"Spam is very lucrative and that is why people along the value chain take their own piece of the pie. With specialisation, you get better at what you do. If you don't have to worry about writing the Trojan, or about running the botnet, your spam content is going to get much better," Weiss argues.

This specialisation is bad news for those in the IT security industry whose job is to stop the spread of spam and malware. "Each one gets better at their task and it becomes

increasingly difficult to defend against," he says.

"These guys are getting so good and what's important about specialisation is that it leads to investigative cul-de-sacs. If I'm just the guy writing the Trojan, you can't follow the whole value chain. It stops with me. Specialisation acts as a barrier to investigation, which makes this mess even more complex."

Spam follows an audience and this helps to explain its recent appearance in places other than just email inboxes. Unsolicited junk emails are now being seen in unlikely locations such as message boards, YouTube pages and Skype instant message chats.

A famous US bank robber, Willie Sutton, was reportedly asked why he robbed banks and his answer was 'because that's where the money is'. A similar principle is at work with online scams, says Weiss. "If you were to chart phishing attacks — the most phished website or bank in the world is PayPal. Why? Because 100pc of their users do online banking," he reasons.

"That's why you get spam on Skype. That's why it's on YouTube message boards. That's why it's probably coming to Facebook. Because millions of people are going there now and it has become a large enough group to target."

There are very good technological reasons why the IT security industry conducts its

own investigations into how spam operations function, Weiss believes. "It's about knowing your enemy. How these guys we're fighting against use internet protocol and how they think and what they're trying to look for: all of those things factor in to the defences."

Information theft is another growing concern for IT security companies. Weiss believes a similar value chain is at work for people looking to steal confidential data. The creator of a program for extracting data from documents may not be the same as the person who gathers social security numbers or credit card details. There is an active market for 'fencing' or trading this kind of information and, as Weiss observes, different people involved at different stages of this process make investigation harder.

Luckily for PC users, the security industry is having some success. IronPort itself was recently involved in an anti-spam pilot project conducted between a coalition of leading European telcos and security organisations.

It's claimed the seven-month initiative resulted in improved spam catch rates. By actively exchanging information between ISPs, especially about spam traffic flows received from one another, the group found a successful approach towards reducing spam.

Email-borne viruses are on

the decline, if the latest statistics are to be believed. Weiss argues that it's wrong to conclude viruses are no longer a threat. Instead, he believes, the battleground has changed.

"The old type of virus would shut down networks and it was something everybody noticed and talked about. Now they're doing it for money, not for notoriety, and the last thing anybody wants is to be detected," he states.

"One of the problems is complacency today in the IT world. I think spyware and malware are just advanced viruses. A virus is something you don't want on your PC and is doing something bad to your PC. Spam is an email that you don't want," Weiss continues.

Seeing the connections between these different threats is the key to managing the problem and preventing users from becoming infected, he adds. "If you were to look at the statistics from WebRoot and others, 80pc of computers are infected with some sort of spyware. That's an epidemic but it's like a silent killer. Nobody's alerted to it because you don't see it happen." Invasion of the PC Snatchers, anyone?

