STOPPING E-MAIL THREATS

PRINT DOCUMENT

ANNOUNCER: Welcome to TechWiseTV on the Cisco Interaction Network. Please remember to submit your technical questions in the field provided at the bottom of the viewing console. You can also email questions, comments, and suggestions, to techwisetv@cisco.com. Thank you for joining us, and enjoy the show.

JONAS TICHENOR: Hello, and welcome to this edition of TechWiseTV, I'm Jonas Tichenor. Spam is big business. Why? Well, because it pays. It has a very low barrier to entry, and very low upkeep costs. Meantime, it's us who are picking up the tab to the tune of about $10 billion a year in lost productivity, consumption of IT resources and help desk costs, and not to mention the increased network capacity the ISPs have to create to carry all that unwanted traffic. And we all know who ultimately pays for that. A war is being fought between those who use email to work, live, play, and learn, and those who see email as a powerful and profitable threat vector. Here's Cisco solutions expert Robb Boyd with a report.

ROBB BOYD: There's no denying that email has lived up to the hype. It's faster, further reaching, and much more convenient, than poor, old fashioned snail mail. But there's a dark side to email, and it's called spam. It now makes up 80% of all email traffic. Why is this stuff so hard to block?

CRAIG SPROSTS: So email, by its very nature, is trusting, it's called the simple mail transfer protocol, and when it was first formed, it was not built with any security features.

DAVID MAYER: In the SIP RFC, security is mentioned over 50 times just in the first few pages. In the SMTP RFC, security is mentioned zero times.

CRAIG SPROSTS: Traditional methods of stopping spam involve two components. Blacklists and whitelists are ineffective simply because the source of spam is changing so rapidly. Content filtering is also ineffective, because it relies on something that spammers themselves can change.

DAVID MAYER: It's literally a spy versus spy environment. Every single time an anti-spam solution comes up with a technique to stop spam, you have armies of engineers, programmers, looking for exploits and flaws to get around that anti-spam tool or technique.

CRAIG SPROSTS: So spam has evolved in three key ways. One is that the source of spam has become much more diverse. So it's no longer a dedicated set of networks, but zombie PCs that are distributed across the world sending it.

PATRICK GRAY: Bot nets are a series of computers that are linked together by a hacker. And what the hacker does is he compromises computers around the world. Strings them together, and it could be hundreds, could be thousands of computers at his beck and call. The bot nets themselves are the pistol, if you will, in the hands of the spammer.

DAVID MAYER: There are dozens of different types of spam attacks out there. Text based spam, image spam, several different variants of image spam. Image spam where you slice and dice the image, where you obfuscate the image with polka dots, or wavy text. There's phishing attacks targeted at specific individuals or organizations. There's image link spam, no text, no image, just a link, click on it, it takes you to the spam.

PATRICK GRAY: We tend to buy solutions, get the box de jour that's going to protect your network from anti-virus. Perhaps an alert, and IDS, or an IPS, that's going to block some of the stuff that's out there. Traditionally, that may have worked, but this is a non-traditional world we live in today. The hacking community is non-traditional.

CRAIG SPROSTS: A few years ago, Bill Gates made the famous quote that spam would be solved in under two years at a conference in Davos. Unfortunately, Bill Gates was not correct about that. Today we estimate that over 75 billion spam messages are sent per day. To put that in perspective, there are only 6.6 billion humans on the planet, so the problem is enormous and growing.

JONAS TICHENOR: I'm now joined live in the studio by Robb Boyd and Jimmy Ray Purser, welcome gentlemen. Now Robb, 75 billion messages a day, how did things get this bad?

ROBB BOYD: Well, it's this bad because there's still a lot of money to be made. There's a book that's recently out, and I was reading about this guy Ed, a reformed spammer, a retired spammer, talks about some of that background. The title of the book is Inside the Spam Cartel, The Secrets from the Dark Side. And he goes into how many infected computers that he could rent. He would actually go to these hackers who would make huge armies of computers, we talked about bot nets, and such like this, he would just rent these for a period of time, and then he would actually receive a commission for how many successful hits he would either get off of those, or sales actually made. And so like any good sales rep, he could log in, and see how much money was coming in, check again, you know, you'd get as much as 50% sometimes on certain pharmaceutical products, things like that. So it's an entire ecosystem.

JONAS TICHENOR: That's unbelievable. It's hard to believe that anyone falls for it. But when you look at the kind of money that these bad guys are making, you know, someone's got to be clicking on these links, and actually applying for these things, getting the meds, whatever they're doing.

ROBB BOYD: Well that's the key, right? I mean, there's many of us, probably anyone that's watching this broadcast has already kind of clued in, and looks like at a lot of things that we get, and they say, how could anybody be clicking on this stuff? But obviously someone is, or it would have gone away. And there's just this talk about the fact that, and studies that have been done, that we are all gullible for a certain extent, we always want something that we can't believe, and they prey on that, right? And so they're going to come after us, and they're going to keep asking for more things. And we could truly get rid of it, if we would remove the economic reasons to do so.

JONAS TICHENOR: Yes, it's the next big stock tip, or whatever, that makes you click on it, thinking I'm going to get someplace that I want to be