Longtime 'Spam King' Charged With Fraud

By Alan Sipress
Washington Post Staff Writer
Friday, June 1, 2007; Page A01

From his 17th-floor Seattle apartment overlooking Puget Sound, Robert A. Soloway allegedly ran an illicit network of computers around the world, secretly commandeering the machines of thousands of unsuspecting bystanders. Prosecutors say Internet users who clicked on infected e-mails and Web sites inadvertently took part in his criminal endeavor: spam.

Soloway, 27, used his empire of hijacked "zombie" computers to send tens of millions of unsolicited e-mail messages over the past four years, prosecutors allege. Described as a spammer since he was a teenager, he allegedly covered his digital tracks using Chinese servers, fabricated Web sites and the purloined identities of hundreds of Internet users whose names and e-mail addresses were slapped on the bulk mailings. He opened and closed bank accounts faster than creditors could track them, prosecutors said.

But federal authorities caught up this week with the man prosecutors call the "spam king" and arrested him on 35 charges of fraud, identity theft and money laundering, casting a light on the byzantine, highly lucrative underworld of mass e-mail marketing. Soloway pleaded not guilty.

"He is one of the bad ones. He's one of the longest-running and uses criminal methods all the time," said John Reid, an investigator with Spamhaus, a European organization that fights spam. "Anyone on the Web for a while would have received one of Soloway's spams."

Spamhaus had included him on its list of the 10 worst spammers until last year, when he was overtaken by more-sophisticated operators, he was overtaken by more-sophisticated operators, but federal authorities caught up with him this week.

http://www.washingtonpost.com/wp-dyn/content/article/2007/05/31/AR2007053100310.html?nav=rss_business
sophisticated operators, primarily in Russia and Ukraine, Reid said.

A lawyer for Soloway could not be reached for comment.

Some forms of bulk commercial e-mailing are not illegal in the United States.

Under the 2003 CAN-SPAM law, which regulates spam, bulk e-mail marketing is allowed if the sender complies with several conditions. Most notably, recipients must be allowed to opt out of the mailings, and the sender must be transparent about the source. Still, scores of big-time spammers have flouted the requirements.

Prosecutors allege Soloway's company, Newport Internet Marketing, defrauded its customers in offering to send a high volume of legitimate e-mail marketing messages or to sell software that could be used in mass mailings. Neither approach performed as advertised but generated a torrent of spam. When customers complained, prosecutors said, Soloway refused to provide assistance or refund the sales, instead threatening to charge them additional fees and refer them to collections agencies.

The scheme went far beyond a deceptive sales pitch, according to prosecutors, who say Soloway used fraudulent Internet practices to drum up customers for his business and then used them to send more spam.

Soloway allegedly used a series of subterfuges to hide his identity and his reputation. Microsoft won a $7.8 million judgment against him in 2005 for sending e-mails that falsely appeared to come from MSN and Hotmail addresses.

Although prosecutors say he has been living in a luxury apartment and driving a Mercedes convertible, Microsoft was never able to collect on the judgment because the company could not locate his bank accounts, Microsoft lawyer Aaron Kornblum said. In a separate case that year, an Oklahoma businessman won a $10 million judgment against Soloway for breaking the law regulating spam but was also unable to collect.

Soloway allegedly masked his continuing involvement by using at least 50 Web site names and registering some of them through Chinese Internet service providers to conceal his involvement. Chinese authorities are less aggressive than their Western counterparts in policing their online service providers and responding to complaints, Internet security experts said. In at least one case, prosecutors said, he stole someone else's credit card information to register and pay for a Web site name.

Soloway allegedly used proxy computers, called zombies or botnets, which were hijacked when the owners opened a software virus embedded an e-mail or Web link. Often, the owners did not realize their computers had been taken over.

Though the indictment does not detail how Soloway first accessed the computers, Internet security experts explained that spammers
often use secret online discussion groups to connect with hackers who lease out networks of zombie computers. Kathryn Warma, the assistant U.S. attorney handling the case, said Soloway used about 2,000 of these zombies at a time and, over the course of his activities, could have taken control of tens of thousands of machines.

By using zombie computers and fake sender names, Soloway was able to ensure that most of his mailings could elude spam filters, prosecutors said. But Warma said this practice amounts to identity theft, and prosecutors are using identity theft laws for the first time to prosecute a spam case. She estimated that "hundreds or thousands" of people could have had their online identities stolen.

"This was a great success by the Justice Department. But this guy is just going to be replaced by one or two or three people in Russia providing the same service," said Craig Sprosts, security analysis manager at IronPort Systems, which sells software for e-mail and Web security. The company reports that 70 billion spam messages are sent daily around the world, nearly double the volume a year ago.
Longtime 'Spam King' Charged With Fraud – washingtonpost.com

Work at Home - Great Pay up to $25-$75 per Hour
www.Retire411.com

Coffee Exposed
A shocking secret coffee co's don't want you to know.
www.coffeefool.com