CNBC.com

E-Mail Spam Falls After Russian Crackdown

TECHNOLOGY NEWS TECH INTERNET WEB SOFTWARE HARDWARE EMAIL RUSSIA

The New York Times | 27 Oct 2010 | 08:23 AM ET

You may not have noticed, but since late last month, the world supply of Viagra ads and other e-mail spam has dropped by an estimated one-fifth. With 200 billion spam messages in circulation each day, there is still plenty to go around.

But police officials in Russia, a major spam exporter, say they are trying to do their part to stem the flow. On Tuesday, police officials here announced a criminal investigation of a suspected spam kingpin, Igor A. Gusev. They said he had probably fled the country.

Moscow police authorities said Mr. Gusev, 31, was a central figure in the operations of SpamIt.com, which paid spammers to promote online pharmacies, sometimes quite lewdly. SpamIt.com suddenly stopped operating on Sept. 27. With less financial incentive to send their junk mail, spammers curtailed their activity by an estimated 50 billion messages a day.

Why the site closed was unclear until Tuesday, when Moscow police officials met with reporters to discuss the Gusev case. The officials' actions were a departure from Russia's usual laissez faire approach to online crime.

They accuse Mr. Gusev of operating a pharmacy without a license and of failing to register a business. On Tuesday, they searched his apartment and office in Moscow, according to Lt. Yevdokiya F. Utenkova, an investigator in the economic crime division of the Moscow police department.

Lieutenant Utenkova said the search of the apartment turned up seven removable hard drives, four flash cards and three laptops. Specific, computer-crime related charges may follow after police examine their contents, she said. The investigation began Sept. 21, six days before SpamIt.com closed.

Mr. Gusev's lawyer, Vadim A. Kolosov, said in a telephone interview that his client was not the owner of SpamIt.com and had never sent spam e-mail, but declined to respond to specific questions.

The drop-off in spam since SpamIt.com went down had been noted by companies in the United States that monitor the Internet.

"We've seen a sustained drop in global volumes," Henry Stern, a senior security analyst at **Cisco Systems**, said in a telephone interview from San Francisco. The company pinpointed the closure of Mr. Gusev's site as the cause for this easing up.

If individual computer users have not noticed changes in spam traffic, it may be because many people have learned to use spam filters that insulate them from the junk that continuously circulates on the Internet.

Kaspersky Lab, an antivirus company based in Moscow, said there had been a notable drop in mass e-mail in the United States that advertised prescription drugs — to about 41 percent of all spam at the end of the September from 65 percent at the beginning of the month. The figures are comparable in Western Europe, the company said. Many of the pharmaceuticals sold through Web sites promoted by spammers are believed to be counterfeit.

Other computer security companies had reported similar reductions in prescription drug spam, although they cautioned that spam volumes were volatile and often spring back to previous high levels. On a typical day, spam accounts for about 90 percent of all e-mail traffic on the Internet.

Mr. Gusev and SpamIt.com have been widely known in computer security circles, and he had lived openly in Moscow. Spamhaus, an international nonprofit that monitors global spam, listed the SpamIt.com organization as the world's single largest sponsor of spam.

Last year, the Russian-language version of Newsweek reported that Mr. Gusev's sites were connected to the same computer server farm in St. Petersburg, Russia, called Russian Business Networks, that was identified in a 2009 report by online security experts with NATO as a source of the attacks on Georgia in 2008.

Mr. Gusev filed suit against Newsweek in a Moscow court, denying links to spamming suggested in the article. That case is still pending. In that suit, he cited phone calls from The New York Times to his lawyer seeking comment as evidence that the article harmed his reputation.

Why, after years of ignoring spammers, Russian authorities have now acted has left online security experts puzzled.

SpamIt.com had operated in a gray area of Russian law, cybersecurity researchers said. They said it had paid commissions to other parties that had directed traffic to various sites operating under the name Canadian Pharmacy, using a Russian online settlement system. Mr. Gusev has denied in blog posts that he promoted spam.

The spammers, meanwhile, operated entirely in the shadows, using networks of computers that had been remotely infected with viruses, known as botnets, and turning them into relay stations for sending e-mail from anywhere in the world.

Some American security experts have said that the spamming operation in Russia appears to have been protected by Russian authorities — whether for reasons of corruption, national pride or state security.

Because most victims of online crime, and the targets of unwanted spam advertising, are in Europe and the United States, Russian police have typically seen little incentive to prosecute online crime, analysts say.

But recently, President Dmitri A. Medvedev of Russia has been seeking to expand and legitimize the domestic Russian Internet industry — and move it away from its reputation as a playground for hackers, pornographers and authors of darkly ingenious viruses.

In June, Mr. Medvedev visited California to meet with Silicon Valley executives. The SpamIt.com site closed two weeks before the reciprocal Silicon Valley trade delegation, led by Gov. Arnold Schwarzenegger of California, arrived in Moscow on Oct. 10.

Computer security researchers have conjectured that spamming gangs have sometimes been co-opted by the intelligence agencies in Russia, which provide cover for the spamming activities in exchange for the criminals' expertise or for allowing their networks of virus-infected computers to be used for political purposes — to crash dissident Web sites, for example, or to foster attacks on foreign adversaries.

The Russian government has denied orchestrating computer attacks beyond its borders.

This story originally appeared in the The New York Times

URL: http://www.cnbc.com/id/39866064/

.

© 2010 CNBC.com