Internet spam and viruses; the missing link

by Jem Berkes [www.sysdesign.ca]

Over the past couple of years, Internet spam and viruses have been a growing menace. This malicious data fills our mailboxes, exhausts the capacity of networks, and poses a significant risk to home users and large corporations alike. While these two Internet-based threats may seem unrelated, there is a very surprising link between the two that has gotten very little press coverage. In this article, I hope to shed some light on this emerging issue.

1st point: Spam is big business

This may be difficult to believe, but spamming can be extremely profitable. As with any other clandestine "business", the people on the front-lines do the dirty work while the people who coordinate the spamming operation make big money. Spammers universally refer to themselves as "Internet marketers", and make their money by overseeing product advertising. If an Internet marketer e-mails an ad to 5 million people, and only 0.1% of the recipients buy the product, this means that a single mass mailing has yielded 5000 sales!

Since it is ultimately impossible for an Internet marketer to conceal their identity while peddling a product to millions of people, a database of major spammers has been compiled over time. The Spamhaus Project (an anti-spam organization) claims that "90% of spam received .. in North America and Europe can be traced .. to a hard-core group of just 200 known spam outfits". The Register Of Known Spam Operations (ROKSO) openly lists the people and companies involved.

However, Internet marketers face a major problem. When they spam directly, they are rapidly tracked down and face retaliation ranging from complaints and harassment to lawsuits. Ultimately, spammers have their Internet connections either suspended or terminated. What once used to be an inexpensive way to mass-market a product has now become very risky business. Spammers, and ISPs that support them, *are not* popular.

Evolution: Spammers find *new ways* to send mail

Spammers figured out a new way to send their e-mails: they would hijack other peoples' computers, and use someone else's resources to perform the mail replication and delivery. While one might think that an Internet marketer would shy away from such a blatantly illegal act, rising levels of spam have proved otherwise. This is currently the primary mode of spam delivery, as it provides anonymity for the true spammer and shifts all the burden to the victim of resource theft.

The most popular forms of resource theft to date have been the abuse of "open relays" and "open proxies". These are servers that have not been properly secured, and which provide varying degrees of anonymity to spammers who use them. These insecure hosts are quickly discovered and blacklisted by system administrators around the world, and pose a diminishing threat.

2003 brings a shift in spammers' tactics

Spammers realized that there was a fundamental problem with their current methods of resource theft: they were trying to adapt to other peoples' software and rely on these unfamiliar systems for mail delivery. There was also a limited number of reliable servers on the Internet that could be abused without being quickly noticed.

Spammers decided to take control of the situation: they could distribute *their own spamming software*, and install it on millions of computers worldwide. After all, a tremendous number of computers around the world now have reliable broadband Internet connections that would be perfect for sending mass mail. A distributed network of spam relays would solve the problem of sender anonymity, and make it very difficult to "shut down" spam delivery.

Spammers would not need anyone's cooperation to achieve their goal. Instead, they started distributing their software in the form of a virus or worm (arriving by e-mail itself, of course) that secretly installs itself on someone's computer. A general disregard for security in consumer software products, coupled with widespread ignorance on the part of users makes it easy to distribute viruses. After all, the great majority of Internet users run the same operating system.

The release of this new 'spamming technology' has been very methodical. The viruses and worms we have seen in 2003 were NOT written by angry teenagers. They were carefully engineered and incrementally released into the wild in a series of tests. The first of the spamming viruses was SoBig; followed by later variants. Each of the tests (a different strain of the same code base) expired on a given date. Spammers released new versions to continue their testing.

New spamming viruses fight back!

Many of these recent viruses are designed to help spammers send out mass mail by hijacking innocent peoples' computers. But there was an interesting development in May 2003; the Fizzer virus carried a component designed to launch a distributed denial of service (or DDOS) attack against certain victims. November 2003 brought Mimail, a new spamming virus also designed to cripple specific Internet targets.

Who are the targets of these attacks? Actually, many of the targets are anti-spam sites I have listed below as references. These are services organized by volunteers that provide mechanisms for highly effective spam filtering. Almost every major ISP relies on services like these to drastically reduce the amount of junk mail their customers receive.

We will likely receive more spam as a direct consequence of these new viruses. The purpose of this malicious software is two-fold: (1) to send spam, and (2) to destroy the most effective mechanisms of spam control we have.

What can we do?

Some would argue that spammers, or “Internet marketers”, are criminals since they gain unlawful access to others' property and use stolen resources for their own benefit. In doing so, they also seek to destroy benevolent organizations that stand in their way. As such, there is growing pressure around the world to aggressively prosecute well-known spammers.

More importantly, spammers will persist as long as people are willing to buy their products. These nuisances are, after all, salespeople. Until the general public realizes how malicious these people are and *stop buying their products*, we will continue to have a major spam problem.

References:

I have learned about these issues through my work developing anti spam and anti virus security software. I have communicated with many system administrators and even some individuals who have been involved with lawsuits relating to spam and Internet advertising. I highly recommend visiting the following URLs for more information:

http://www.spamhaus.org/ and http://www.spamhaus.org/rokso/
http://www.spews.org/
http://spamcop.net/
http://groups.google.ca/
Search for “spammers release virus”
Search for: “news.admin.net-abuse.email”
http://www.spamlaws.com/