Spam flitters

I was going to write about complex systems this month but I've spent much of it investigating various spammers who recently decided to borrow my company's name with which to bombard the world with invitations to purchase a crappy watch, (does anybody take this seriously), or to stock up on medicines guaranteed to interfere with body chemistry in unusual ways.

We are of course not alone in this. Many genuine companies are regularly abused in the same way. The first intimation you get is when hundreds of undelivered messages show up reflected back to you with unlikely names like "CarmenTheMyopicSlug@throbbing.co.uk". I tracked down the source of these to a fixed set of IP addresses in China and Korea and contacted my own ISP. Regrettably, they explained that very little can be done about this apart from request that the ISPs of the spammers concerned check their logs and intervene which we both duly did. Fat chance. They haven't responded to any of our requests. I experimented with automatically returning all undelivered messages to one of the spammer's own sites so that they spammed themselves. This made me feel a little better but it doesn't achieve anything in the long term so if anybody has any really good ideas about dealing with this permanently, I and thousands of others would like to hear. Automatic filtering can make most of the problem invisible but goodness knows what percentage of web traffic is taken up by this stuff. On our systems, about 99% of what we receive is correctly intercepted by our anti-spam filters and binned.

Let me name names or rather IPs. The following are all engaged in large scale spamming: 221.5.2.37 (China) is a royal pain in the URLS whilst 221.11.134.38 (China) and 222.122.63.28 (Korea) are multiple offenders. The spammers typically cycle through aliases to these every couple of days. Whether it would do any good if we all complained to the ISPs who tolerate this is unclear.

The month finished with a few Paypal scams. First off the blocks was a pathetically crude attempt to convince me that somebody called Nola McFadden wants to send me money via Paypal. A little analysis reveals that this is intercepted by http://www.ermacisza.ro/.temp/paypal.com who would like to soak up your details before ripping you off blind. They had numerous attempts this week under various unlikely names. Thank you Romania, you can forget my Eurovision song contest vote. Meanwhile http://freebsd.chues.tpc.edu.tw/~kids/ would like to convince me my Paypal account has just been suspended. Thank you kiddies. Its a little more upmarket than the "I AM DE DAUGHTER OF DA LATE MINISTER ... AND MY LEFT LEG HAS JUS BEEN NORRED OFF BY A MAD CHEETAH ..." but not much. While they are this bad I don't suppose we have too many problems but the way it stands currently, you might as well junk everything that comes from .cn, .ro, .tw or .pl until they do something about it. Mine are 100% scams.

Finally, given all the warnings about ignoring all e-mails from Banks, who should e-mail me this week about deals but the Bank of America. A phone call confirmed that it was legitimate. I sometimes don't know why I bother. Perhaps they've mistaken a CIO as a Chief Insecurity Officer.

lesh@leshatton.org