Blog for TrustSphere

http://www.trustsphere.com/ipv6-better-for-spammers-worse-for-you/

IPv6: Better for spammers, worse for you?

Posted on August 13, 2012

There's a major change occurring on the Internet which is weakening existing defenses against email spam.

We know the ever-growing numbers of cell phone users necessitated the creation of new local area codes. And as more and more mobile devices offer full Internet access, the number of assignable IP addresses—which enable computers to talk with each other--has likewise dwindled. This led to Internet Protocol version 6 (commonly referred to as IPv6). Launched worldwide just this past June, IPv6 essentially utilizes more complex 128-bit coding to exponentially increase the number of available IP addresses now and into the future.

The bad news about IPv6 is that most existing methods of spam detection are about to be rendered virtually obsolete. Spam can often be detected by *content filtering*—scanning for specific suspect phrases ("discount prescription meds", "fake Rolex", etc.). The main drawback of content filtering is that it frequently leads to "false positives"—legitimate emails routed into the spam folder.

A more precise method has been *blacklisting*—recording and blocking IP addresses of known spammers. But with the number of IPv6 addresses now closer to infinity, a spammer can now easily acquire a much larger chunk of multiple "dummy" IP addresses, effectively evading—if not overwhelming--blacklist databases. It's like trying to catch a single raindrop in a thunderstorm.

For major companies and other large-scale enterprises, the big-name security products on the market today—reliant on content filtering and blacklisting--will still be there. They weren't perfect before, and are even less perfect now. We continue to recommend a *trusted sender recognition* solution as the bedrock of any corporate email security matrix. It's "reverse engineering" of the alternatives, and entirely future-proof. Give it a look here.