Sunday, August 19. 2007

Spam

So, i hope that the changes to the infrastructure will lead to an more stable website. So, what it´s the problem: 3000 Visits a day are really good for a niche blog like c0t0d0s0.org, but normaly nothing near a problem for Apache. The problem: The useful requests aren´t the problem. Within twelve hours this weblog gets round about 100.000 hits. The bandwidth consumption is between one and two gigabytes per day. And most of it is spam: Within 12 hours the script for posting comments was triggered 78000 times. 78000 useless requests, 78000 useless request to spam filter clearing houses.

When i started as an architect at nordwest.net 10 years ago, we´ve designed the systems for 50.000 pageviews a day. Now i need 50.000 pageviews capacity without having served a single reader of my blog. Something goes really wrong in the internet.

The problems isn´t the internet itself. The problem starts in Redmond: My ruleset for the worst spam offenders (100 and more comment requests within the last 12 hours) is 50 lines long. 50 different IP addresses. 50 different systems. As long it´s so easy to "own" other peoples machines and aggregate them to bot nets, there will be no escape from this.

By the way: Microsoft can´t give itself a green image as long their are not able to secure their operating systems. Millions of Millions of CPU cycles are wasted every day for cleaning up the problems of an operating system never meant to be connected to a network. Companies operate large arrays of systems to filter spam in every form of its existence, searching for viruses on dozens of attack vectors. Home users operate firewalls, the mail programms use compute intensive heuristics to search spam and scan for scamware, virures, malware, ransomware and so on. Now think about computing without all this. Without the possibility to use large bot nets, a simple ACL in your router would suffice. A secure operating system from Microsoft would be the most efficient energy saver right now ....

Posted by Joerg Moellenkamp in English at 12:17

Jörg,

we have not even seen the problem, the SPAM war just has started.

A single T2000 can filter a few hundred messages per second. Our brightmail-bundle may help here (which is also the reason why we at Sun internally do not have these amounts of SPAM, because we use Symantec brightmail on T2000s). Ask you provider to install T2000s with Brightmail and your problems are gone.

Rgds,
Frank
Anonymous on Aug 19 2007, 17:01

Mailspam is only a single attack vector ... Trackback Spam, Comment Spam, Wikispam and so on ...
Anonymous on Aug 19 2007, 21:25

I can see your problem.
I've disabled comments on my blog.
Then, the spammers started to use trackback spam, and I had to install SpamKarma2, just to get rid of the trackback spam!
I didn't even really know what a trackback was. I just wanted to have a blog and a website to upload some digital pictures...

The ball is clearly sitting in Redmond - but there's no easy solution. As long as the supply of idiots clicking on anything that comes as mail-attachment (or popup in a web-browser) is seemingly infinite, the problem will persist.
Instead of trying to get the users educated, these guys have spent billions to de-educate and dumb-down "users" of even the simplest principles of information-technology.
Now, the world get's the (energy) bill.
Thanks, Bill.
Anonymous on Aug 20 2007, 03:25