

modusNews

Vircom Europe's Newsletter

"The catch and false-positive rates are so excellent that it's simply amazing. Thanks Vircom!"

**Kai Fiebach
Musikhochschule Lübeck,
Germany**

June 2006

Dear Partners,

Here is the question to ask to your customers and prospects:

Is your anti-Spam solution really "good enough" ?

In today's battle against Spam and Phishing, most corporate customers have implemented some protection. Some use recognized solutions and start to believe that the spam problem is so heavy that having some spam messages getting through is still "good enough".

But is it *really* ?

New spammers techniques

Last month, the volume of spam surged by 20% and the number of new zombies – infected desktop PCs, located all over the world, that spammers secretly hijack to relay their emails – increased by about the same amount.

IMAGE SPAM

Image spam, an increasingly common and sophisticated network nuisance, is difficult to catch because email filters cannot "read" messages embedded in an image. Spammers, therefore, easily bypass filters by sending a unique, slightly different image each time.

BOTNETS

Lately, spammers started to combine image serialization, with the use of millions of spam zombies or "bots". This makes them even more difficult to catch:

- Bot networks make it difficult to block spam based on senders IPs (RBLs...)
- Serialization makes it difficult to block spam based on signatures

Anti-Spam Efficiency

Several months ago, the average efficiency of good anti-Spam filters was about 93%. Since about 70% of today's emails is spam, this means that each mailbox still receives about 5 spam messages for 30 valid emails. For a company of 500 mail users, this daily "left through" rate represents a productivity loss of about 14.000 €/year!

For those who do not like numbers, imagine the impact of a security horn ringing everyday for more than 20 seconds, annoying and distracting all (even so protected) employees...

The problem is getting worse. The overall number of spam messages grows continuously, and new techniques, like the ones described above, decrease filters' performances even further.

There is another aspect that pledges for higher efficiency: the new threat landscape is shown to be increasingly dominated by attacks and malicious code that are used to commit cybercrime.

With Phishing on the raise (today about 1% of all Spam messages) and adult spam still getting the highest hit rate (a recent study showed that 5% of adult-related spam that reaches end users' mailboxes is opened by recipients), cybercrime gives corporations even more vital reasons to improve their catch rate.

So, with Modus' consistent 98+% catch rate with less than 0,01% false positive, ask your customers and prospects...

✔ What was your Spam threshold before buying an anti-Spam solution ?

✔ What will be your "left through" threshold before switching to Vircom ?

New Pricing

We are launching today a new price list. It is much easier to use and as always provides the best value for money in the market !

Here is a short version of it:

Modus AS (includes Perimeter Defence, anti-Phishing, anti-Spam & Sieve-based Policy Management)

SME Product (50 - 249 Mbx)
Standard Edition (250 - 999 Mbx)
Enterprise Edition (1000 - 5000 Mbx)
Large Scale Edition (> 5000 Mbx)

Price per Mbx	
Product	Renewal
13,00 €	6,50 €
8,00 €	4,00 €
5,00 €	2,50 €
Ask for Quote	

Options

Integrated Norman anti-Virus
Integrated McAfee anti-Virus
Integrated Norman & McAfee Bundle
Appliance (Requires Norman anti-Virus)

Price per Mbx	
Product	Renewal
2,00 €	1,00 €
5,00 €	2,50 €
6,00 €	3,00 €
3.750,00 €	750,00 €

Success Story

Winning against GFI, Barracuda and Ironport

A new partner, say NewVAR¹, referred one of their customer to us, say MediumCUST¹, a 1.000 Mbx customer who was in a bind. A new virus or spam was circulating on the Internet using MediumCUST's email domain as spoofed source (i.e. the email from field was *@mediumcust.com).

The target email servers were sending hundreds of virus warnings and bounce notices back to MediumCUST.

They were using two email gateways (GFI MailEssential and a nameless email relay) in front of their Exchange server. The quantity of email traffic, and the way these emails were being processed, brought down to a crawl both email gateways, in effect paralyzing the email infrastructure of the customer. Although the Exchange server remained operating, emails could not be received because the gateways were flooded.

We got the reference from NewVAR in the morning and by noon, we had spoken to the customer and diagnosed with him what the problem was. The customer did not have any performing hardware available to install software, so we proposed to show up at his office with an appliance. By 4pm, we were on site, installing the appliance. An hour later, the other two gateways were removed, and email was flowing smoothly. The ModusGate Appliance was weathering the storm without breaking a sweat and allowing legitimate through.

The customer was about to cancel his business trip scheduled for the next day, as he could not figure out how he was going to get out of his bind. He was so impressed by 6pm that he decided to leave and monitor the appliance remotely. Performance has been outstanding since.

In the following weeks, the customer had to go through the company's purchasing process and get bids from competitors. He received quotes from a local, open-source base hosted solution, Barracuda and Ironport. We faced some challenges with each; we beat the current solution (GFI), the hosted offering and Barracuda on quality and Ironport on pricing.

One can use many angles in this case:

- 1) Great support for a channel partner's customer in distress
- 2) Upsized competitive displacement vs. GFI
- 3) Beat two well established appliance vendors (Barracuda & Ironport)

¹ At this stage we can not yet publish their names. Call us for further details.

