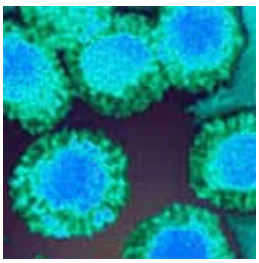
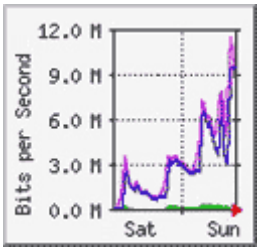
# Virus and dDoS Attacks on Spamhaus



In June 2003 Spamhaus warned that spammers had progressed from spamming through open proxies to actually manufacturing and sending out computer viruses, infecting hundreds of thousands of business and home-user machines on broadband (ADSL) lines, in order to create a vast network of anonymous spam 'zombies'.




Virus DoS traffic hitting one of the Spamhaus web servers following the release of the W32.Mimail.E virus on Saturday 1 November.

On November 1st 2003 a virus codenamed W32.Mimail.E began infecting hundreds of thousands of Microsoft Windows computers worldwide. Like other Trojan worms before it, W32.Mimail.E is designed to install a malicious program (in this case "foo.exe") which rifles through the user's address books sending itself onwards to every email address it finds, whilst harvesting the addresses for the spammers who sent it, but there the similarities with previous Trojans worms end because W32.Mimail.E's job once installed, is to begin attacking the Spamhaus website, www.spamhaus.org.

Two days later, on 3rd November 2003, a second virus codenamed W32.Mimail.H was released. It too conducts a distributed Denial of Service (dDoS) attack on www.spamhaus.org.

On December 1st 2003, yet another MiMail virus W32.Mimail.L was released, like the others it too conducts a dDoS on www.spamhaus.org, but it also goes further. W32.MiMail.L claims to come "From" a spamhaus.org address 'billing@spamhaus.org' and the message the virus delivers is designed to provoke the biggest reaction possible from millions of victims: the Subject of the virus email is "We are going to charge your credit card". The message tells users that unless they respond by emailing a spamhaus.org address, Spamhaus "will bill your credit card for amount of $22.95 on a weekly basis. Free pack of child porn CDs is already on the way to your billing address."

In early 2003 spammers, crackers and virus writers joined forces to launch the first known spam virus, W32.SoBig.E, a Trojan designed to infect computers worldwide to create an arsenal of proxies/zombies through which spammers could send billions of spams anonymously. Up to 60% of all spam is now sent using virus-infected computers.

While SoBig was the most famous spam virus, a more sinister virus known as Fizzer was released before it in May 2003 by a now known group of spammers into "porn & pills" spamming, dDoS cyber-attacks and credit card fraud. Fizzer (W32.HLLW.Fizzer) is a wide-spread Trojan worm which spreads by emailing itself to contacts in Microsoft Outlook and Windows address books. The purpose of Fizzer is to install a minature web server (on which spammers then host rapidly-moving "porn & pills" web sites linked to from spams), an IRC backdoor enabling the spammer to control the infected machine, and a DoS attack tool specifically for attacking anti-spam organizations.

As spam from virus-infected computers soared in mid 2003, spammers began using their new armies of infected 'zombies' to mount attacks against anti-spam systems including Spamhaus which stood in the way of them spamming millions of Internet users.

Beginning in early July 2003, Spamhaus servers came under massive distributed Denial of Service (dDoS) attacks by thousands of virus-infected computers throughout the Internet. Over the course of the summer we sustained massive dDoS attacks from 2 different spam gangs, but survived thanks to our large distributed network capable of absorbing the attacks, and thanks in no small part to the engineering skills of the server administrators running Spamhaus' servers. Other anti-spam systems weren't so lucky, during August and September 2003, four anti-spam systems were forced into closure under overwhelming dDoS attacks.


dDoS attacks on Spamhaus continued for much of July and August 2003 with ever-increasing intensity. In September, expecting more attacks, Spamhaus moved its web servers behind an anti-dDoS device known as **iSecure** supplied by Melior CyberWarfare Defence. iSecure has kept the dDoS attacks at bay.