MessageLabs

Email security intelligence report

January-June 2004

Spam

Between January and June 2004, MessageLabs' Anti-Spam service scanned a total of 5,006,942,923 emails.

Of these, 3,181,672,070 were identified as spam.

This equates to a percentage of 63.5%, or 1 in 1.57.

The monthly breakdown is as follows:

June 2004:	86.3%, or 1 in 1.2
May 2004:	76.0% or 1 in 1.3
April 2004:	67.6% or 1 in 1.5
March 2004:	53% or 1 in 1.9
Feb 2004:	60% or 1 in 1.7
Jan 2004:	63% or 1 in 1.6

In comparison, during the first six months of 2002, MessageLabs' Anti-Spam service identified 1.5% or 1 in 67 of emails scanned as spam. In 2003 during the same period, this figure had jumped to 37.9% or 1 in 2.6.

Spam headlines

June 2004 An AOL engineer is arrested and charged with stealing and selling AOL's entire customer list to spammers. A complaint filed in federal court charged the engineer and list buyer with conspiring "to send massive amounts of unsolicited commercial emails — also known as spam — to millions of AOL's customers." It is alleged that approximately 92 million email addresses were traded.

June 2004 MessageLabs breaks the news that spammers have started using spyware to automatically send personal information about a PC user back to spammers, who then use that information in the subject line of subsequent spam emails. By using familiar words and phrases in the subject line, such as passwords, a pet's name, or a company name, it is hoped that users will be more likely to open the email.

May 2004 The US Federal Trade Commission announces that spammers are required to label spam as sexually explicit if it contains pornographic images. The penalty for non-compliance is a heavy fine. The new rules follow the CAN-SPAM Act and are designed to shield computer users from exposure to unwanted sexual images. Given spammers disinclination to send "honest" email, it surprises few people that most have chosen to ignore this ruling.

Viruses

Between January and June 2004, MessageLabs' Anti-Virus service scanned a total of 5,623,252,284 emails.

Of these, 467,995,469 contained a virus.

This equates to a percentage of 8.3%, or 1 in 12.

The monthly breakdown is as follows:

June 2004:	1 in 10 or 9.3%
May 2004:	1 in 10 or 9.1%
April 2004:	1 in 10 or 9.5%
March 2004:	1 in 43 or 2.3%
Feb 2004:	1 in 19 or 5.1%
Jan 2004:	1 in 129 or 0.1%

During the first six months of 2002, MessageLabs' Anti-Virus service identified 0.3% or 1 in 392 of emails scanned as containing a virus.
In 2003, during the same period, this figure had increased slightly to 0.5% or 1 in 208.

Virus headlines

March 2004 The creators of the Netsky and Bagle worms go head-to-head in an Internet battle with Bagle authors including abusive messages in their code. Some Netsky worms were also programmed to delete copies of several variants of the Bagle worms when detected on infected machines. Numerous iterations of the Bagle and Netsky worms were released during the first half of 2004, with hundreds of thousands of copies intercepted by MessageLabs to date.

March 2004 In a new twist, some versions of the Bagle worm attempt to spread via password-protected Zip files. While some traditional anti-virus vendors announced that they had introduced methods of dealing with this, MessageLabs had been able to protect against this technique for some time. Skeptic, MessageLabs' unique predictive technology, is capable of searching for the appropriate

password within an email and using that to unlock and scan the Zip file for malicious code.

January 2004 The new year begins with a bang when the first of the MyDoom worms burst on to the scene. MessageLabs intercepted an unprecedented 1.2 million copies of the worm during the first 24 hours and the worm achieved a peak infection ratio of 1 in 12 emails. As with the majority of viruses released so far this year, MyDoom.A incorporated a backdoor element and create a network of compromised machines that could be used as spam relays. The worm also launched a successful denial of service attack on the website of The SCO Group.

Phishing

Between January and June 2004, MessageLabs intercepted a total of 1,529,040 phishing emails (emails containing a URL to a fraudulent website).

This breaks down as follows:

June 2004:	264,354
May 2004:	247,027
April 2004:	205,953
March 2004:	215,643
Feb 2004:	259, 014
Jan 2004:	337,050

Phishing headlines

May 2004 In one of the first reported cases of a phisher being identified and charged, Michael Maloney, a 17-year-old from New York, was accused of sending emails claiming to be an official communication from AOL. He faced charges from the US Federal Trade Commission (FTC). The phishing emails contained a link to a fraudulent website designed to look like the official America Online site. Victims who clicked the link and filled in the personal details were in fact giving sensitive banking and credit card information to potential cybercriminals.

May 2004 Gartner publishes findings from an April survey of 5,000 US online adults and shows that 57 million or 41% of US adults have or think they have received a 'phishing' attack email. Of 141 million online adults, more than 30 million or 19% stated that the email that they received "definitely was a phishing attack." According to Gartner, more than 1.4 million users have suffered from identity theft fraud, costing banks and card issuers $1.2 billion in direct losses in the past year.

Email security trends and developments during the first six months of 2004

Convergence

The predominant email security trend during the first half of 2004 has been the fusion of email security attack methods – commonly known as convergence. The virus and spam landscapes have changed dramatically, and virus writers and spammers are combining their skills to produce a more sophisticated breed of email security threat.

Examples of this trend are the viruses that have been designed to aid the spread of spam.

These include Fizzer, Bugbear, and the SoBig and MyDoom worms. Of the viruses that have been intercepted by MessageLabs since January 2004, almost all have been found to have the potential for spam distribution.

Whilst it is impossible to say for certain why the boundaries between viruses and spam have been eroded, one potential explanation seems more likely than any other – money. There is little or no monetary profit to be gained from simply distributing viruses, but when you combine the capabilities of a virus and the profit that can be earned from spam, suddenly you have an altogether more materialistic proposition.

The rise of the online fraud scam

Just one year ago, the phishing phenomenon was relatively unheard of – in August 2003, MessageLabs intercepted just 14 phishing-related emails. By January 2004 this number had climbed to more than 337,000 – a worrying upsurge.

In June 2004, the number was 264,354. These online fraud scams involve the use of viruses, spam, spoofed websites and social engineering techniques. The purpose of phishing is clear — to defraud organisations with a significant online

presence and their customers out of considerable sums of money.

For companies used as the bait in an attack the impact is primarily on their brand and reputation, but increasingly phishing is a financial burden. Phishing also presents numerous legal liabilities related to violating consumer privacy and the protection of sensitive information.

Phishing has occurred on every major English-speaking continent. In North America, customers of TD Canada Trust, Citibank, Ebay's PayPal and Visa have unwittingly divulged account numbers, passwords and other confidential information. The story is similar in the United Kingdom, where customers of Barclays, NatWest, Lloyds TSB and Halifax responded to false emails citing online banking problems. Customers of the four main banks in Australia (ANZ, Westpac, National and Commonwealth) have also been targeted by phishing scams.

Sender authentication

Industry players are looking at new ways to beat spam. One such development is sender authentication — a way to check that an email has genuinely been sent from the domain it claims to come from. It works by examining the IP address of the email — if it does not match the source of email as given by the domain, it is likely to be a forgery.

Sender authentication is not designed to prevent spam per se — it is a way of finding out whether an email has been "spoofed". However, given that many spammers re-route their spam and forge its origin, authentication should help to weed them out. It should be noted that identifying forged emails has implications for phishing scams and the spread of viruses too.

Initially there were three main technologies offering sender authentication — SPF (Sender Policy Framework), created by pobox.com, DomainKeys from Yahoo!'s and Microsoft's Caller ID. Two of these have since merged — SPF and Caller ID, now known as Sender ID. More detail of this collaboration will be discussed at the IETF meeting in August.

Despite some opponents (resistance is coming mainly from those involved in the design of email who are reluctant to break existing specifications) sender authentication is likely to gain mainstream support. Will sender authentication spell the end of spam? Alone, probably not — anti-spam technology will still have an important part to play. But it should turn out to be a significant piece of the puzzle.

Spam — international co-operation and enforcement

On July 2, representatives from the United States, the United Kingdom and Australia signed a Memorandum of Understanding (MoU) that called for improved law enforcement cooperation among the three countries to ensure better enforcement of anti-spam laws. The three countries have agreed to permit enforcement authorities to cooperate on spam investigations, engage in training programmes to improve investigative abilities, work toward international solutions and develop new ways to tackle spam and improve cross-border enforcement of spam laws.

While there is no doubt that the MoU was needed, multinational cooperation may be impeded by the different approaches taken in each country. The MoU itself recognises that the laws of the three countries vary "substantially." For example, spam that is illegal in the UK may be legal in the USA and Australia. Consequently, the cooperation will only function on a "lowest common denominator" approach, ie: only when spam is considered illegal in all three countries and only in the most "serious" cases of spamming.

Nonetheless, the MoU does have the kernel of a very useful tool even if, for the moment, it is restricted to a level of cooperation most citizens would assume and expect from their governments. If international cooperation could be extended to ensure rapid communication between network operators and ISPs whose servers are being hacked or compromised, it would be an improvement over current conditions. Similarly, if parties cooperate to shut down compromised home PCs that are being used to relay spam and carry out denial of service attacks, international cooperation could lead to reductions in global spam.

• For more information on MessageLabs Intelligence and the analysis provided, please visit: www.messagelabs.com/intelligence

About MessageLabs Intelligence
MessageLabs Intelligence is a respected source of data and analysis for email security issues, trends and statistics. MessageLabs provides a range of information on global email and security threats based on live data feeds from our control towers around the world. The information relating to MessageLabs' services contained in this report, is based on data generated internally by MessageLabs and has not been subject to an independent review by a third party.