MessageLabs Intelligence
Annual Email Security Report
2004

-The year the big phish was landed-

Contents

Introduction

The following MessageLabs Intelligence Annual Email Security Report is a round up of the email security trends and developments of 2004. It analyses the spam, virus and phishing landscapes and provides MessageLabs' predictions for 2005.

In summary, viruses and spam have largely been regarded as the two main email security threats faced by businesses. They have dominated the email security landscape, and the convergence of the two has presented a particularly potent threat. Yet at around this time last year another, equally sinister threat was stirring.

At the end of 2003 few people had even heard of phishing. Yet within a relatively short period of time, the phishing phenomenon had gathered enough momentum to establish its position as one of the most prevalent threats of the day. In September 2003 the number of phishing emails encountered by MessageLabs was 279, by September 2004 that figure had jumped to over two million.

Currently, MessageLabs intercepts between two and five million phishing emails every month. The impact of phishing is also evident in the Email Security Survey carried out by MessageLabs in May 2004, when the majority of respondents (22%) claimed that online fraud would be the greatest threat over the next decade. There is little doubt that 2004 was the year of the phish – and it's here to stay.

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 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.

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

About MessageLabs

MessageLabs is the leading provider of managed email security services to businesses based on market share. The company offers industry-leading managed Anti-Virus, Anti-Spam, Image Control and Content Control services to more than 10,000 businesses around the world to combat email threats before they reach corporate networks and without the need for additional hardware or software.

Powered by a global network of data centres spanning four continents, MessageLabs scans tens of millions of emails each day on behalf of clients such as The British Government, The Bank of New York, Bertelsmann, CSC, Diageo, Random House, SC Johnson and StorageTek.

The service is also available through more than 600 channel partners, including BT, Cable & Wireless, CSC, IBM, MCI and Unisys.

For more information on MessageLabs, please visit www.messagelabs.com.

Email security trends and developments during 2004

1) New phishing tackle

In addition to the increasing volume of phishing emails in 2004, the perpetrators of online fraud scams have also developed more complex and sinister techniques over the course of the year. Typically, phishing attacks require users to click on a URL within an email, which appears to have come from a legitimate bank or e-commerce site, then enter personal account details into a fraudulent website, putting them at risk of identity theft.

However, more recent phishing emails are designed to capture online banking details automatically when a computer user opens the email. Towards the end of October, MessageLabs intercepted a number of emails that silently run a script when opened, attempting to rewrite the host files of targeted machines. Some of the emails were completely blank. The next time the user attempted to legitimately access online banking they were automatically redirected to a fraudulent website, where their log in details could be stolen.

Only three Brazilian banks and their customers were targeted by this scam at the time, but successful execution of the scam could lead to increased adoption of the technique.

In another twist, MessageLabs discovered in November that phishers were attempting to recruit middlemen by luring unsuspecting victims into laundering money and exposing them to possible identity theft. The emails offered regional representative and general assistant positions with a legitimate organisation whose name was used in an attempt to lend credibility to the scam.

Examples of the main organisations targeted by phishing scams during 2004 include Citibank, HSBC, eBay, Visa, Natwest, ANZ and Westpac

2) Spammers – is the net closing in?

A number of spammers have been arrested and/or convicted during 2004. One of the most famous cases was that of Jeremy Jaynes and Jessica DeGroot, who were convicted for offences related to spamming in November. In June, officials arrested an AOL employee for allegedly stealing personal details relating to millions of AOL members that were sold to spammers. During the same month, a Texas woman named Jennifer Murray was indicted and arrested for violating Virginia's anti-spam law in the US.

Since the introduction of anti-spam laws around the world, several arrests have been made. The implementation of the laws themselves has done little to curb the tide of spam on a global scale, indicating that spammers believed that they would not be caught and charged. It rapidly became clear that implementation would be key, and the subsequent arrests have been important in demonstrating that spamming is a crime, and will be dealt with severely.

One of the most successful spam laws to date is the Australian Spam Act that went into effect in April 2004. Offering fines of up to $AU1.1 million a day until the spammer stops, the Act has seen a significant decrease in spam activity by the country's spammers, who have been keeping a low profile, many appear to have almost ceased activities and at least one is known to have left the country.

Although it would be naïve to expect spammers to give up their day jobs, it is hoped that high profile arrests and stringent spam laws will convince some of them to change careers. The most determined however may decide to transfer their business to countries like China and Russia, out of the grasp of current legislation.

3) The plague of the virus variants

A major trend of 2004 has been the seemingly endless number of variants of particular viruses. Depending on the vendor you reference, W32/Bagle.AZ, W32/Netsky.AE, W32/MyDoom.AJ and W32/Mimail.V have all been seen throughout the year. There are a number of potential reasons for this. One of them being that virus code is often released into the public domain, making it easy for copy cats to use as the basis of their own creations.

There is another more sinister reason for the continual stream of reincarnated viruses and worms. Virus writers are aware of the window of vulnerability, and know that they have a period of time during which no software-based protection exists against new malware. To take advantage of it, they create malicious code designed to spread as far as possible in the shortest period of time, thereby infecting the greatest number of machines.

The fact that in a few hours signature files will be released and machines will be updated is irrelevant to the perpetrators – because they already have another variant lined up. By changing the make up of the virus slightly, they are able to circumvent identity files that have already been released. For the anti-virus software vendor, it's back to the drawing board, and so the cycle continues.

4) The sender authentication saga

Sender authentication is designed to prevent the spoofing of email addresses by checking whether 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.

Initially there were three main technologies offering sender authentication - SPF (Sender Policy Framework), created by pobox.com, DomainKeys from Yahoo! and Microsoft's Caller ID.

Following the Internet Engineering Task Force's rejection of Microsoft's Sender ID proposal, in October it disbanded its MTA Authorization Records in DNS (MARID) working group. MARID was originally formed to develop a standard approach to address the sender authentication problem. Instead of adopting Sender ID as a standard, the proposal remains "experimental."

Another blow was dealt when AOL announced that it had "serious technical concerns" with Sender ID, and that it would only use SPF for checking inbound mail for its subscribers. With a fundamental lack of agreement over the technology to be used, the future of sender authentication remains unclear, but the creation of a unified standard will probably be left to the vendors as they continue to develop their own approaches.

One of the advantages of using a managed service is the provider can take responsibility for managing the implementation of any sender authentication scheme. Also, a managed service is more likely to benefit from economies of scale afforded by such a system.

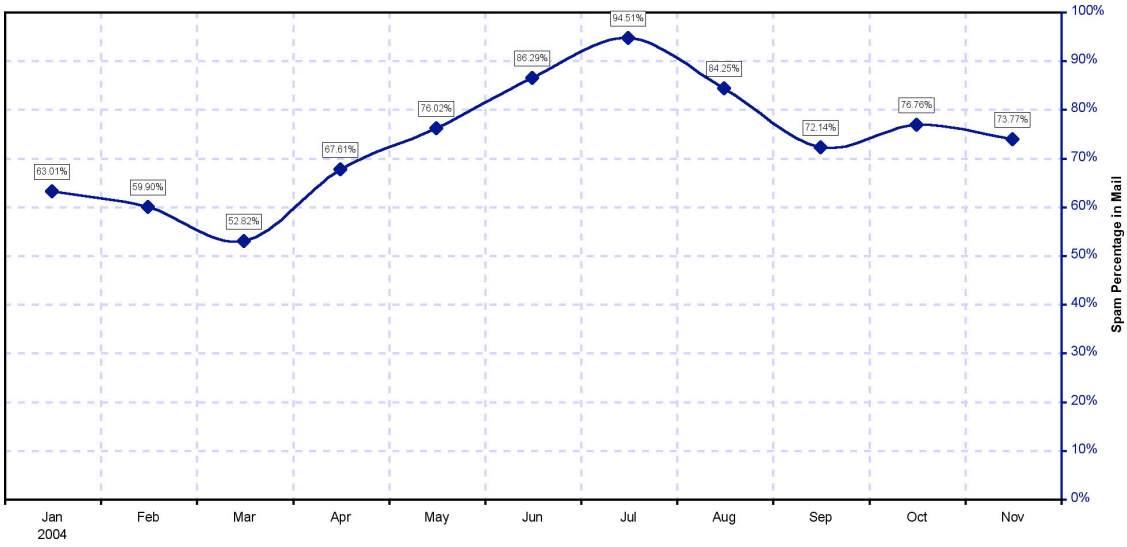
Spam, virus and phishing statistics

1) Spam Statistics

During 2004, MessageLabs Anti-Spam managed email security service scanned more than 12.6 billion emails. Of these, more than 9.2 billion, or 73.2% (1 in 1.4) were identified as spam.

The monthly breakdown of spam on a global scale is as follows:

November	73.8% or 1 in 1.4
October	76.8% or 1 in 1.3
September	72.1% or 1 in 1.4
August	84.2% or 1 in 1.2
July	94.5% or 1 in 1.1
June	86.3%, or 1 in 1.2
May	76.0% or 1 in 1.3
April	67.6% or 1 in 1.5
March	53% or 1 in 1.9
Feb	60% or 1 in 1.7
Jan	63% or 1 in 1.6



These figures show that over the course of 2004, the overall trend has been an increase in spam volumes, as predicted at the beginning of the year. The first few months show a steady rise, culminating in some sharp peaks in June and July. Since that point, the volumes have reduced but are not as low as at the start of the year.

Spam volumes are likely to continue to vary month on month, according to a number of factors including spammer arrests, introduction of more stringent spam acts, user awareness and the impact of new technologies. Over the next year MessageLabs expect spam volumes to remain in the 60% – 90% bracket depending on external factors.

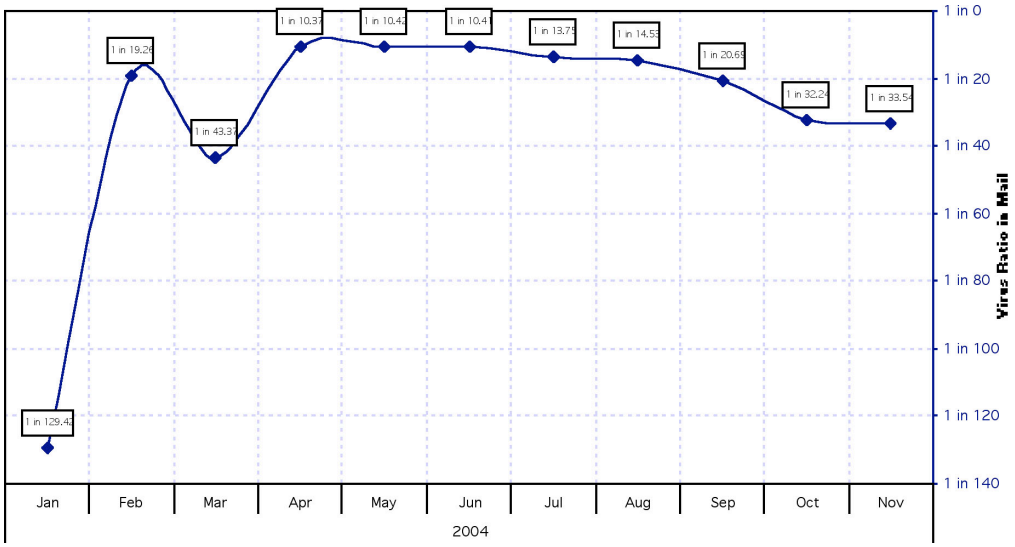
By comparison, during 2003, MessageLabs Anti-Spam service identified 40% or 1 in 2.5 of emails scanned as spam. In 2002 this figure was 9% or 1 in 11.

2) Virus Statistics

MessageLabs Anti-Virus managed email security service scanned a total of 147 billion emails during 2004. Of these, 901 million or 1 in 16 (6.1%) contained a virus.

The monthly breakdown of viruses is as follows:

November	1 in 33 or 3.0%
October	1 in 32 or 3.1%
September	1 in 21 or 4.8%
August	1 in 15 or 6.9%
July	1 in 14 or 7.3%
June	1 in 10 or 9.3%
May	1 in 10 or 9.1%
April	1 in 10 or 9.5%
March	1 in 43 or 2.3%
Feb	1 in 19 or 5.1%
Jan	1 in 129 or 0.1%



The ten most widespread viruses of 2004 were:

1. W32/MyDoom.A
2. W32/Dumaru.A
3. W32/Swen.A
4. W32/Sobig.F
5. W32/Mimail.J
6. W32/Bagle.A
7. W32/Klez.H
8. W32/Sober.C
9. W32/Mimail.A
10. W32/Mimail.I

Similar to the spam volumes, the number of emails infected with a virus during the course of the year has increased overall, with peak activity during months toward the middle of the year – April, May, June and July.

This is not surprising given the convergence between spam and viruses. The majority of viruses are designed to install open proxies on infected machines, allowing them to be used for spam distribution. It therefore makes perfect sense for periods of high virus activity to coincide with, or slightly precede, rises in spam volumes.

Unlike spam, outbreaks of viruses can have a major impact on overall virus numbers. For example, the jump from January to February is due to the effects of MyDoom.A, and the high ratios in spring and summer as a result of the Netsky/Bagle war.

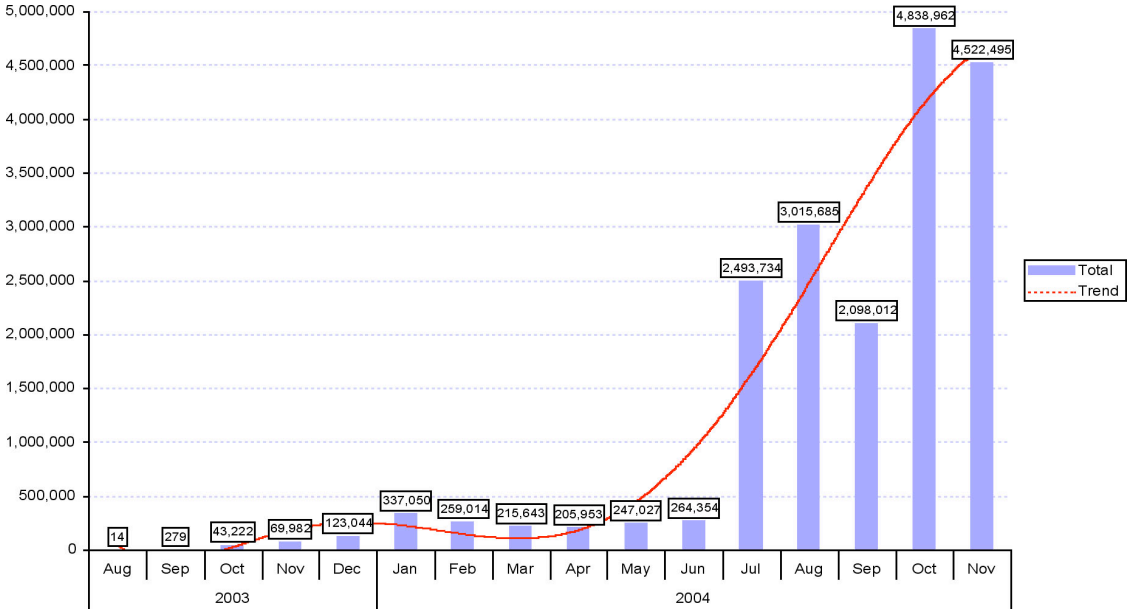
In comparison, during 2003 MessageLabs Anti-Virus Service identified 3% or 1 in 33 of emails scanned as virus infected. In 2002 this figure was 0.5% or 1 in 212.

3) Phishing Statistics

During 2004, MessageLabs intercepted over 18 million phishing emails (emails containing a URL to a fraudulent website).

The monthly breakdown of phishing emails is as follows:

November	4,522,495
October	4,838,962
September	2,098,012
August	3,015,685
July	2,493,734
June	264,354
May	247,027
April	205,953
March	215,643
Feb	259, 014
Jan	337,050



The number of phishing emails intercepted by MessageLabs during the first half of the year remained fairly stable, and was generally between two and three hundred thousand per month.

However, as the popularity of phishing scams began to soar in July, so have the figures – the number rose by almost two million from June to July and did not drop significantly since for the rest of the year.

At its peak, MessageLabs intercepted almost five million phishing emails in October 2004. Phishing made a huge leap in the middle of 2004, and there is every reason to believe that the numbers will climb further during 2005 as phishers find new social engineering tricks to lure unsuspecting victims.

Email Security News

November

Spammer convicted to nine years in jail

Two spammers were convicted of three charges of sending thousands of junk emails through servers in Virginia, USA. Jeremy Jaynes, rated the world's eighth most prolific spammer, was sentenced to nine years in prison and his sister, Jessica DeGroot, who had used credit cards to purchase domain names for spam distribution, was fined $US7,500 (£4,075).

The indictment stated that over 10,000 spam messages were sent during several twelve-hour periods, and that they forged transmission and routing information to prevent victims from finding out who the sender was and how to contact them.

It is hoped that high profile cases such as this will help to deter spammers.

October

Mass-mailing viruses could be a thing of the past

Experts at the Virus Bulletin Conference in Chicago in the US presented research suggesting that if anti-virus vendors were able to reduce the window of vulnerability, or signature delay time, to three hours or less, virus outbreaks would be all but eliminated. Unfortunately, current analysis shows that the anti-virus software community has only managed to reduce the window of vulnerability from 12 hours to 10 during the past year.

The window of vulnerability is the delay between the appearance of a new email-borne virus or worm, and the release of signatures by traditional anti-virus software vendors. Customers of managed email security vendors such as MessageLabs are not subject to signature delay times, owing to the use of predictive technology capable of detecting previously unseen viruses.

September

Click to become a zombie

MessageLabs researchers identified emails containing a click to opt-out link designed to turn machines into open proxies, which can be used for distributing further spam. The drag-and-drop JavaScript exploit took advantage of an Internet Explorer bug to download an executable file when the mouse is scrolled across the malicious domain page, allowing the machine to be controlled remotely.

Further, once the executable had been loaded, remote attackers could upload new Trojans at any time, leaving machines vulnerable to key logging and password capture.

August

Microsoft's sender authentication proposal rejected

The Internet Engineering Task Force rejected Microsoft's contribution to the authentication standard, Sender ID. The decision was taken because of Microsoft's intention to impose certain restrictions on the use of the system, specifically its plan to keep a possible patent application secret. Microsoft stated that anyone using the technology must take out a license, and many in the open source community stated that this was too restrictive. There were also concerns over possible incompatibilities with open source software.

Days after this decision, AOL announced that it would not be supporting Sender ID either due to "lackluster" industry support and compatibility issues with Sender Policy Framework.

Operation Slam Spam lands spammers in the slammer

Dozens of people were either arrested or charged with crimes related to spam, identity theft and other computer crime offences. The cases were brought by law enforcement offices around the US, and were developed by a team of federal law enforcement officials and representatives from industries reliant upon the Internet.

The operation built a database of known spammers, drawing from law enforcement agencies and private companies that are investigating and bringing civil suits against some of the biggest senders of junk email. It also used online decoys to catch spammers and purchased products advertised in spam so that financial records could be traced to the ultimate source of the message.

This crackdown is thought to be the biggest yet.

Phishing attacks overtake virus outbreaks

Despite the fact that phishing is a relatively new phenomenon it has gathered significant momentum over a relatively short period of time. Analysis performed by MessageLabs comparing phishing and virus outbreaks shows that the impact of certain online fraud scams is comparable to and in some cases exceeds the prevalence of virus outbreaks.

In one example, a phishing attack directed at a well-known US bank and its customers generated 125,000 emails within the first five hours of its appearance. In contrast, only 23,000 copies of the high profile MyDoom.O worm were stopped within the first five hours of the outbreak.

March

DTI survey reveals infection despite protection

A survey conducted by the Department of Trade and Industry in the UK revealed that 68% of large companies suffered a virus infection in 2003 despite the fact that 99% had anti-virus software products in place. Although some organisations reported little or no damage as a result of the infection, others claimed that an attack had resulted in costly clean ups and disruption that continued up to a month afterwards.

The findings added fuel to the argument that, used in isolation, anti-virus software is not a sufficient defence against infection, due primarily to its reactive nature. A common view is that signature-based protection is fundamentally flawed due to the need to issue a new signature for every new virus or variant. Often anti-virus software vendors are only alerted to the fact that a new virus is in the wild by a customer or another vendor. By this point it is too late to protect those organisations hit in the first wave of the attack.

As a result of the failings of traditional anti-virus software, many companies are adopting proactive managed services capable of detecting known and unknown viruses at the Internet level, before they can enter the network.

January

The outbreak of the year

The New Year began 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 during 2004, MyDoom.A incorporated a backdoor element and created a botnet (a network of compromised machines that can be used as spam relays). The worm also launched a successful denial of service attack on the website of The SCO Group.

To date, MessageLabs has encountered 23 variants of the MyDoom worm.

2005 Predictions

1) Business on the front line – email security attacks get personal

In 2004 MessageLabs encountered evidence of email attacks tailored to one or a small group of organisations. These ranged from blackmailing online gambling sites to avoid denial of service attacks, to threats of sending out child pornography in the name of a particular organisation if they refused to pay the perpetrators. MessageLabs has also seen Trojans and other malicious code designed specifically to compromise certain organisations.

Until this year, security attacks tended to be random and used scattergun approaches to finding victims. Given these examples, it is possible that criminals could soon start tailoring threats and techniques that make a big impact on specially selected targets.

2) Compliance and regulation

Compliance-driven demands are expected to grow in importance during 2005. In recent years, various laws have been introduced that require tighter controls over financial reporting and disclosure, prompting businesses to develop policies for monitoring and archiving business transactions – including email and instant messaging.

The most notable ones are the Gramm-Leach-Bliley Act, the Health Insurance Portability and Accountability Act, Sarbanes-Oxley, SEC Rule 17a-4 and NASD Conduct Rules 3010 & 3110. These each affect email administration and archiving. Although introduced in the U.S., they have been partially embraced by companies in France, Germany and northern Europe. Asia Pacific countries such as Japan and Singapore are beginning to adopt similar approaches.

The consensus now suggests that emails that can be construed as business records should be retained for certain periods. Archiving every message may be considered the safest way to go to be compliant, but with volumes of email traffic, spam and instant messaging, this approach proves costly and creates challenges in keeping message systems running effectively.

A failure to comply with regulations creates risks to a company's credibility and reputation and can result in legal action.

These regulations are already leading to increased spending on email management and security services. Email management solutions can help companies establish, enforce and monitor policies and create safer working environments, thus helping them to avoid falling foul of these laws. Any solution that blocks spam, viruses, phishing scams and pornographic content can also cut bottom line costs and increase system availability.