



# MessageLabs Intelligence: April 2006 Catch Me If You Can: A Review of Quarter 1/2006

## Introduction

Welcome to the April edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for April 2006 to keep you informed in the ongoing fight against viruses, spam and other unwelcome content. This is also the first MessageLabs Intelligence report of 2006 to take a retrospective look at the events which have helped shape the security landscape over the past few months.

Highlights from this report include:

- Spam – 58.5% - Up 0.7 % (last month it was down 2.8%)
- Viruses – 1.5% - Down 0.2% (last month it was down 0.9%)
- Phishing - 0.28% - Down 0.05 % (last month it was up 0.02%)

The US was the main source of malware, spam and phishing attacks, hosting 18.1% of world's compromised computers in Q1 06, however these levels could be perceived as low compared to Q2 05 when levels were at an all time high of 43.92%.

India received a welcome break from the spamming world this month; it happily fell from the 3rd highest victim in March with 59.1% to the lowest in April with just 18.5%.

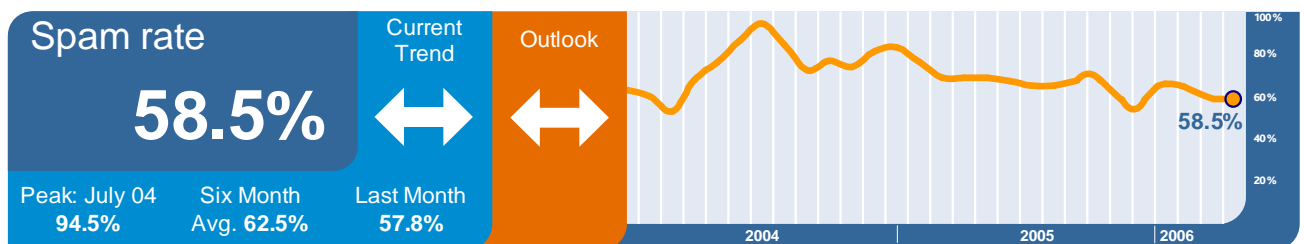
Although phishing levels have been on the decline during 2006 (1 in 356.2 in Q1 compared to 1 in 279.8 in Q4), phishing is expected to rise in the coming months due to the increasingly targeted nature of phishing attacks, known as spear-phishing.

Business Support Services continues to be the vertical victim for both spam and virus attacks, with the largest monthly increase of virus attacks – 1 in 5.4 emails heading for this vertical now harbor a virus or some form of malware.

## Global Trends & Content Analysis

MessageLabs Anti-Spam and Anti-Virus Services focus on identifying and averting unwanted communications originating from unknown bad sources and which are addressed to valid email recipients.

**Skeptic™ Anti-Spam Protection:** In April, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 58.5% (1 in 1.7), an increase of 0.7% on the previous month.

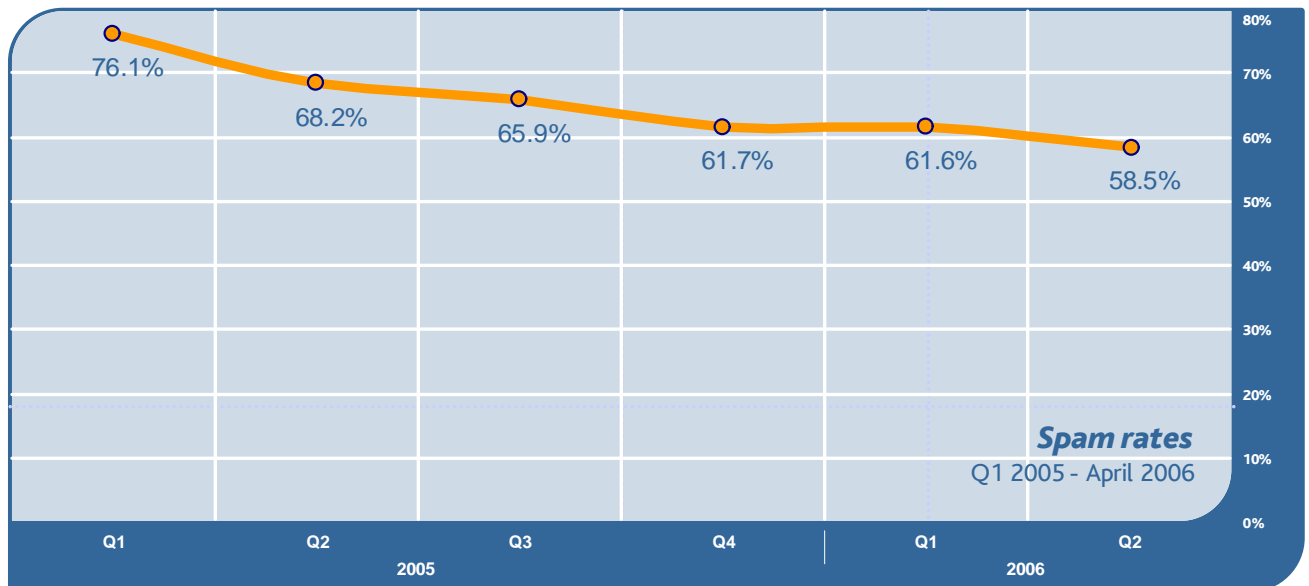


The core spammers are essentially those that make up the SpamHaus ROKSO top 200 list, which remains almost unchanged from a year ago. However, there have been a few notable differences.

For example, “Nigerian 419” spammers have appeared a lot more in Eastern Europe and Russia than they had previously. These spammers don’t generate large volumes of spam, but what they do can be harder to detect because it looks more like a regular email with no embedded links, and are often sent from legitimate web mail systems and cyber cafes, which cannot be easily block-listed.

**Quarterly Review:** From the chart below, it can be seen that spam levels intercepted by MessageLabs for Q1 are not as high as the same period in 2005. This suggests that spam concentrations have reached a plateau, however, this does not show the proportion of spam that is much easier to filter, for example from known botnet sources.

Overall, real spam levels have not actually changed much since the same period 12 months ago. Without the additional measures capable of filtering this detritus at the internet level and making it more difficult for spammers to reach MessageLabs clients, 82.9% of email traffic would be identified as spam. For further information, please see the section on Traffic Management in this report.



In the coming months and over the next year, it is essential that governments establish clear anti-spam policies and provide enforcement authorities with greater powers to achieve any effective results in tackling spam, which is increasingly becoming an obstruction for developing countries with emerging economies that depend upon the internet for e-commerce.

In April, the Organization for Economic Cooperation and Development (OECD) finally launched its Anti-Spam Toolkit. This is the culmination of almost two years effort by the organization’s Anti-Spam Task Force, first established in August 2004. In calling for governments and industry to try and do more to tackle the problem of spam, this new set of OECD recommendations have been developed and include recommendations on cross-border co-operation in the enforcement of laws against spam.

**Spyware – From Botnet Boom to “Busted!”**

In January 2006, we learned from the latest FBI Computer Crime Survey that almost nine out of ten U.S. organizations experienced computer security incidents last year and that viruses (83.7%) and spyware (79.5%) headed the list of attacks, accounting for a loss of around \$12 million.

Last month saw the extradition of an Israeli couple accused of developing spyware used for corporate espionage. The

highly specialized trojan software was discovered to have been used by ruthless private investigators working for a number of Israeli businesses, in order to gather covert information on their competitors.

The case originally came to light last year, when the trojans were being sent to carefully selected businesses via an email attachment purporting to be a business proposal, in order to trick users into downloading the spyware. Well-known businesses, including TV, mobile phone, car import and utility companies were accused of using this malware, which was developed by the couple, to steal rivals' corporate secrets and monitor their activities.

Spyware is an increasingly pervasive and growing problem. In a survey conducted by NCSA and AOL last December, 61% of computers were discovered to have some type of spyware or adware installed on them, with less than 10% being installed with the owner's knowledge or permission.

Spyware can provide a very lucrative revenue stream for the growing number of criminals who have control over increasing numbers of robot networks (or "botnets"). With no regard for the victim, using such "drive-by-installs", a cyber criminal can make several thousand dollars by remotely installing adware on the compromised PCs enslaved under their control, all without the owners' knowledge or permission. Each installation may often only generate a few cents worth of revenue, but for someone with control over a large botnet, these revenues can increase significantly. Once installed, the adware is difficult to remove and provides a means of delivering targeted pop-up advertisements, based on personal data harvested from the user's online browsing habits.

More concerning perhaps are the malicious worms that are used to create these botnets, which are capable of gathering far more sensitive information from the users' machines, including cracked usernames, passwords, credit card numbers and other personal data stored inside their web browser's auto-fill database. With this level of intelligence, the fraudsters are able to target their attacks even more effectively with the knowledge of which sites the bots under their control regularly access.

In April, spyware again received the attention of the long arm of the law. In the U.S., the New York Attorney General has brought a case against a well-known adware company, allegedly linked with software that many users don't even know is installed on their computers. This software is always meant to be installed with the permission of the users, but many unscrupulous affiliates of adware companies have been installing the software regardless. It seems that advertisers are still liable if any link in their chain of affiliates, and sub-contractors is found to have acted illegally. Speaking at a lecture in New York last month, Ken Dreifach, an attorney in the New York State Attorney General's office said, "You don't want to ever assume that the existence of intermediaries, whether it's two or six, is going to immunize you from liability."

The distribution of adware online is reportedly a multi-billion dollar industry, fuelling a boom in the number of botnets that are now being created. In January this year, Jeanson James Ancheta (aka "Resili3nt") pleaded guilty to charges brought by the FBI for installing adware on a botnet of more than 400,000 compromised PCs.

During the court hearing, Ancheta admitted that he earned around \$60,000 in fees as an affiliate for surreptitiously installing adware on to his large botnet. By staggering the installations, Ancheta avoided detection by the advertising companies who paid him for each installation.

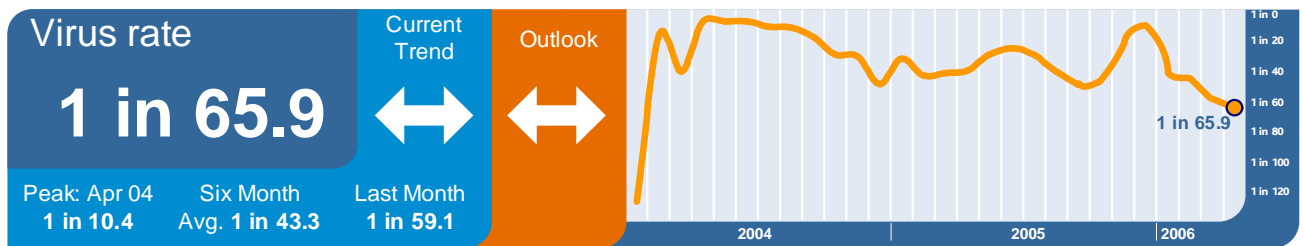
In the first case of its kind in the U.S., targeting profits from the use of botnets, sentencing is due in May; but under plea yet to be approved, Ancheta may serve between four and six years in prison, possibly forfeiting a 1993 BMW and over \$58,000 in profit. He is also expected to pay costs of around \$15,000 to the U.S. government for infecting military computers.

**Skeptic™ Anti-Virus and Trojan Protection:** The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources destined for valid recipients, was 1 in 65.9 (1.5%) in April, a decrease of 0.2% since March.

In April, Microsoft responded to the widely publicized CreateTextRange() vulnerability by including a patch in the company's April "Patch Tuesday" update. One of the concerns around this particular flaw is that it came to light only a few weeks earlier, in late March. This bug soon became a popular target for hackers who were reportedly able to create hundreds of malicious web pages exploiting the flaw to take control of vulnerable computers visiting these sites.

Among the patches released by Microsoft in April were a number for the Office suite of applications. It has become more important now for users to patch these applications as well as the operating system. In recent months the number of attacks targeting application vulnerabilities has increased since applications are not patched as regularly as Windows itself. Such targeted attacks occur when criminals send Word documents to carefully selected business email addresses which contain a malicious payload that may remain undetected by traditional anti-virus software.

No longer satisfied with “playing” with Windows, in recent weeks users of Apple Macs have received a wake-up call in the shape of a number of specifically crafted worms that target the ostensibly secure Mac OS X operating system. Perhaps this is more indicative of the niche hackers who are finding it increasingly difficult to create an unsavory reputation for themselves in the wake of such widespread criminal domination of the Windows malware space, and are finding some respite in the hacking of Mac OS X.



**Quarterly Review:** In Q1, virus and trojan traffic declined slightly from the end-of-year high of 1 in 28.9 (3.46%), representing a drop of 1% compared with the same period in 2005, of 1 in 41.8 (2.39%).

The general trend of fewer large-scale outbreaks continues (with the notable exception of Nyxem at the end of January).



**Agility over Fragility – Changing the Nature of Outbreaks**

Large scale virus outbreaks have almost become a thing of the past, as attacks are increasingly more targeted. In contrast, on January 16th MessageLabs intercepted more than 4 million copies of Nyxem.E (aka MyWife.D, BlackWorm or Kama Sutra) from over 150,000 unique IP addresses during the first week alone.

Recently we have become more accustomed to malware being seeded by botnets. This is characterized by a sudden influx of malware, going from zero to many thousands an hour – almost instantly. However, Nyxem had a different pattern,

starting slowly and taking several hours before it became significant, suggesting that a botnet was not used to seed this particular outbreak, rather a more old-fashioned approach of using spam to propagate the worm, or posting the malware to newsgroups on the internet.

Although seven vendors were able to detect this new strain heuristically –making a judgment based on the properties of the code and what it was trying to achieve, rather than through a signature – many anti-virus vendors were unable to provide protection for at least 4 hours, and in one case up to 35 hours (according to av-test.org).

There then followed a two-week window before the virus was due to activate its destructive payload on the 3rd of each month, and begin corrupting files on infected computers. On the face of it, Nyxem was a flashback to the days before cyber criminals dominated the landscape and much of the malware around had been the internet equivalent of joyriding.

During this two-week window, Nyxem recorded its reproduction effort on a particular website counter, and provided a rare opportunity for security companies and ISPs around the world to track information about the spread of the virus. A concerted global effort could also be made to clean-up the infection before the virus would strike on the critical date. In the final week, MessageLabs tracked over 11,000 computers worldwide being disinfected each day.

CAIDA, (the Cooperative Association for Internet Data Analysis) also published their analysis of the Nyxem IP address data and estimated that between 400,000 and 900,000 computers in more than 200 countries were affected by Nyxem, and that around 45,000 were also infected with other forms of botware or spyware. More than 84 per cent of the infections were on broadband connections, and around 30 percent of the infections were in India.

In the days following the 3rd February, reports of several thousand computers in India being damaged by Nyxem were already starting to surface, which is also marked in MessageLabs own statistics in this report, when in the months following the attack, spam and virus traffic for India have skyrocketed.

Although Nyxem provided some unique insight into the extent of an otherwise fairly lackluster virus, other more dangerous viruses with criminal aspirations tend to propagate more rapidly, and are often more widespread and don't draw too much attention to themselves. This is evidenced in the first quarter of 2006, which has also witnessed a number of other sequels too; besides Nyxem there have also been a number of new strains of the now infamous Bagle worm.

New Bagles usually begin life as a new downloader component, often undetected by traditional security software, posted to one of the compromised websites continually being monitored by already infected computers. Bagle has evolved from the early strains which comprised a fairly monolithic executable that was mass-mailed in email outbreaks, to a fairly sophisticated malware application suite. In one of these recent strains, we saw a return to "polymorphism" – the ability for a virus to change its attributes to better evade detection – the executable code in this case was being repacked repeatedly on the server to create a different version of the same program each time.

Other strains of Bagle also discovered this quarter were found to include a "rootkit" component. A rootkit is a mechanism that allows the virus to conceal itself from the operating system and security software installed on the infected computer, making it very difficult to identify and remove.

More concerning perhaps is the fact that rootkits aren't new, and Bagle isn't the only family of "botware" to employ rootkit technology, but the technology is appealing to more and more cyber criminals especially if it can help safeguard their botnets from traditional anti-virus software. Moreover, Microsoft Research has recently been interested enough in rootkit technology to develop its own state-of-the-art rootkit prototype, called SubVirt, presumably in order to gain a better understanding of the criminal mind and to create better security counter-measures.

**Bot Review:** When investigating the source of much of the malware, spam and phishing attacks, the U.S. fosters the majority of the world's compromised computers. In the first quarter of 2006, 18.1% of the world's zombie computers were found in the U.S.

It can be seen from the following chart that in April (Q2), this figure dropped slightly to 16.92%, with China not far behind, with around 16.47% during the same period.

Although not shown on the below chart, in recent weeks South Korea has seen a resurgence of attacks aimed at taking

control of the country's high-bandwidth domestic broadband computers, with 2.12% of the bots located in the country at the end of Q1 2006. This isn't as high when compared with 6% for the same period in 2005, but this number is expected to rise further.

According to a recent survey released by the OECD, broadband adoption in the U.S. rests in 12th position internationally despite having largest total number of broadband subscribers with 49 million.

Iceland has also overtaken South Korea in this latest survey with 26.7 broadband users per 100, as compared with 25.4 users per hundred in South Korea. However, the OECD further suggested that this may be a temporary stumbling block as the country begins to transition to the next generation of fiber-based broadband, which grew by 52.4 percent during 2005, according to the report.

The following chart shows the breakdown of compromised computers, including botnets, around the world that have been responsible for distributing the majority of the malware and phishing attacks intercepted by MessageLabs.

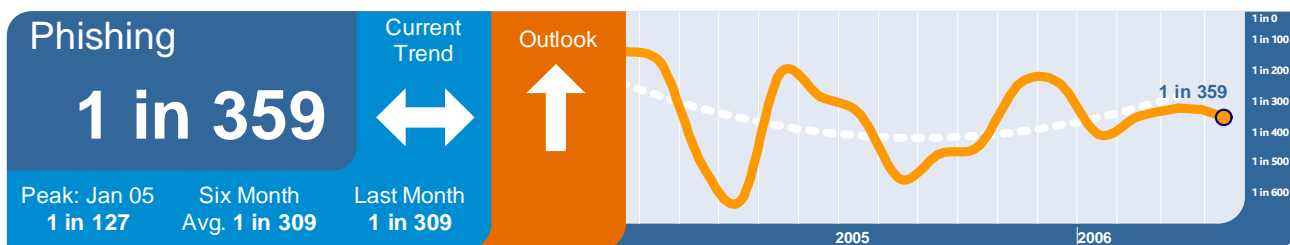
	UNITED STATES	CHINA	GERMANY	INDIA	UNITED KINGDOM	FRANCE	ITALY	TURKEY	BRAZIL	JAPAN
<b>2005 All</b>	22.47%	16.07%	13.17%	8.60%	9.47%	9.15%	7.10%	5.10%	4.94%	3.94%
Q1	11.39%	26.04%	1.04%	8.14%	17.60%	4.44%	4.29%	1.04%	21.15%	4.88%
Q2	43.92%	20.74%	1.97%	8.27%	4.20%	5.42%	3.06%	1.67%	7.41%	3.32%
Q3	20.06%	18.33%	9.93%	7.91%	11.18%	9.35%	7.86%	4.71%	5.86%	4.82%
Q4	23.56%	14.30%	15.84%	9.11%	8.39%	9.12%	6.67%	5.48%	4.21%	3.31%
<b>2006 YTD</b>	17.94%	14.86%	12.11%	13.02%	8.96%	8.43%	6.42%	9.57%	4.35%	4.33%
Q1	18.10%	14.61%	12.52%	12.62%	8.91%	8.46%	6.51%	9.74%	4.31%	4.22%
April	16.92%	16.47%	9.46%	15.57%	9.29%	8.23%	5.87%	8.51%	4.60%	5.08%

When investigating the distribution of compromised computers around the world, just what is being seeded by a botnet and what may be originating from an infected computer is sometimes difficult to differentiate.

For example, a botnet may initially be seeding a variant of Mytob (which contains bot technology), but after a number of iterations this seeding will probably stop and all that is left is the mass mailer component which continues to self-replicate. In another example, Bagle, it is quite possible that the same computer will be broadcasting more than one Bagle variant; a lot of Bagle malware doesn't actually self-replicate, rather it is spammed-out, so when we do find such a computer, it is probably being used by a machine that is part of the Bagle botnet.

The going rate for renting a botnet at the moment is roughly \$50-60 per 1,000 to 2,000 bots, but it rather depends on how the bots are to be used, in some cases the price may be higher. For example, a fraudster who has developed a bank stealing trojan, but no distribution network may expect to pay a bot herder to install the trojan on some of the machines in his network, and sometimes the bot herders expect "extras," i.e. they will monitor what their bots are doing when they are hired out and log any credit card numbers, personal data, etc. that may be collected or relayed through them.

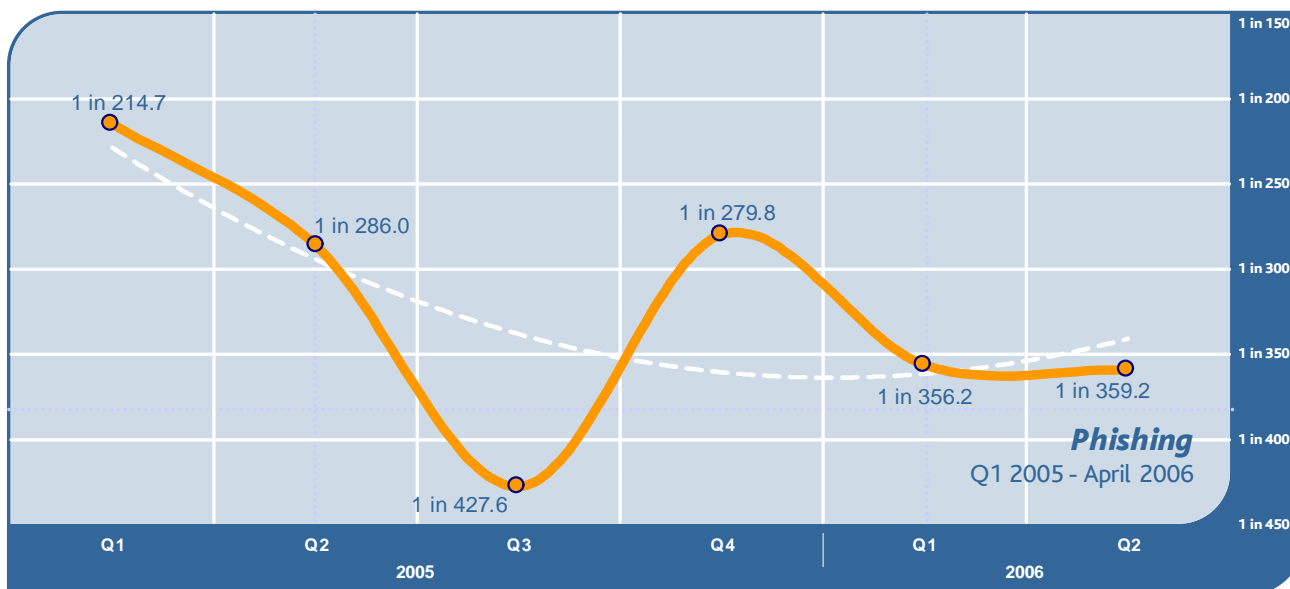
**Phishing:** April showed a decrease of 0.05% in the proportion of phishing attacks compared with the previous month. One in 359.2 (0.28%) emails was a phishing attack. However, the number of phishing attacks has increased by 1.1% as a proportion of all email-borne threats, now accounting for 15.6% of all malicious emails intercepted by MessageLabs in April.



In March, it was being widely reported in the U.S. that a number of phishing scams spoofing the U.S. Internal Revenue Service (IRS) were in circulation in the run-up to the April 15th deadline for filing tax returns. The IRS were sufficiently worried to publish an alert about the scams, describing how it had identified 12 sites in 18 countries that were being used to bait U.S. citizens into revealing personal data and potentially to trick them in to installing malware capable of compromising their computers. MessageLabs did see a number of these purported emails, however, not on the scale that seemed to be widely reported at the time.

**Quarterly Review:** When we look at the quarter-on-quarter trend over the last year, we can see that in spite of the recent decline, phishing is expected to rise in the coming months, although perhaps not to the same levels as were observed in Q1 2005. This is due in part to the increasingly targeted nature of phishing attacks.

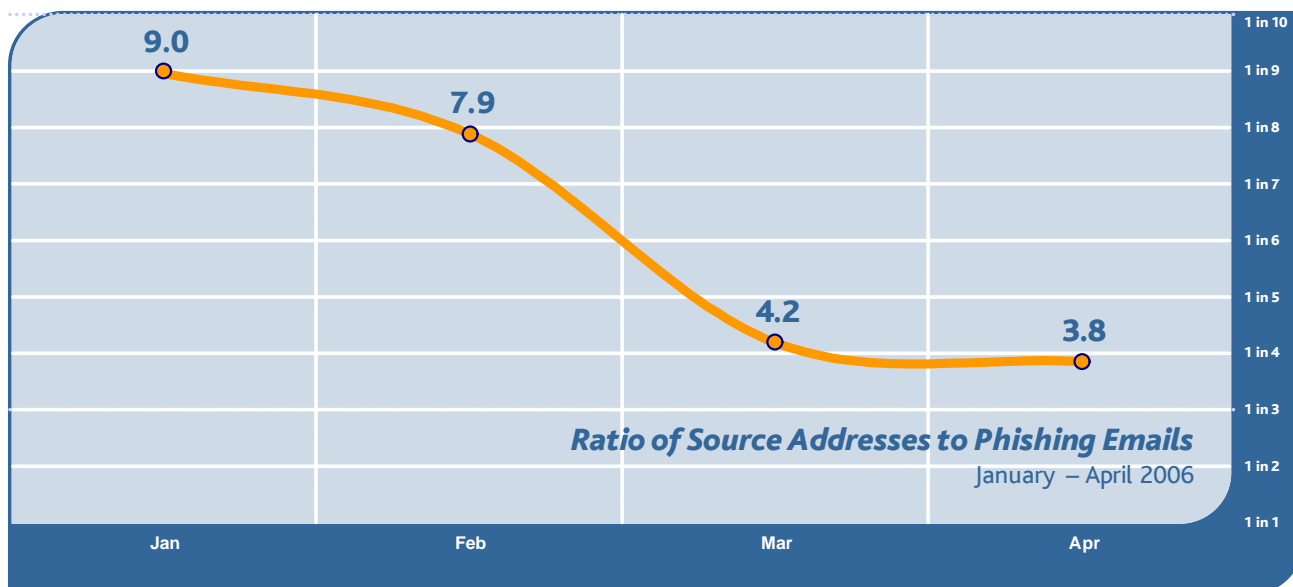
MessageLabs has continued to observe a decline in the scatter-gun approach where phishing emails used to be sent in large numbers. In recent months, more and more phishing attacks are being distributed in batches, and one problem with attempting to track phishing scams is that they are often sent out from compromised web servers using PHP based mail scripts, as well as botnets under their control or rented for the purpose.



With this, fraudsters and botnet controllers are now being more conservative with the use of their botnets and favoring greater numbers of more discreet botnets; individual phishing sorties are now much smaller than they were only a few months ago.

From the chart below, it can be seen that during a phishing attack, each compromised computer is not being used as aggressively as earlier in the year. For larger botnets, this number falls further still. For example, in April, one particular attack was broken into a number of smaller runs, each comprising between 100,000 and 200,000 emails, but each bot would be used to send only 5 or 6 emails.

The profile for a similar attack in January would have each bot broadcast an average of 8 to 12 emails, from a botnet of between 20,000 and 30,000 computers.



The reason for this is that although overall phishing levels haven't changed a great deal in Q1, the number of bots under the control of cyber criminals has increased. As a consequence, the ratio of phishing emails per bot has dropped by more than half, from an average of 9 in January, to an average of 3.8 in April, i.e. each compromised computer will on average be used to send out fewer than 4 emails per phishing run.

#### **“Spear-phishing” Increases In Popularity**

As attacks become more targeted and phishing attacks more selective, it can be perceived that some lessons have been learnt from the malware community, where the collateral damage created by a large virus outbreak often contributed to its swift discovery and demise. By reducing the amount of “noise” from an attack, phishers are simply focusing their attacks on selective groups of addresses which allow for a higher probability of success than that of spamming huge numbers of emails with very low hit rates.

By improving the structure and content of these phishing emails, and reducing the size of an attack – and even by targeting employees of a particular bank or organization, they can significantly improve their chances of success with a targeted “spear phishing” sortie. Prospecting email addresses from the internet that contain certain target domains is relatively easy, and many companies are now adopting a multi-layered approach to security, including internet level filtering extending their defenses beyond the network perimeter, as well as providing more security training and raising awareness of such attacks internally.

#### **Banking on a Fortune From Phishing – the Banks Fight Back**

In April, the German federal crime agency (the BKA), released information about an operation targeting an international criminal gang engaged in identity fraud. The BKA had been monitoring the gang since the end of last year, following an investigation into some alleged phishing activities. Each phishing email contained a trojan that collected the bank account details of its victim. When caught, it is believed that the gang had already managed to launder tens of thousands of Euros from German bank customers which were then siphoned into Eastern Europe.

Another similar case involved the extradition from Argentina of a Spanish hacker alleged to be responsible for the loss of millions of Euros from Spanish banking customers from phishing attacks. José Manuel García Rodríguez (aka “Tasmania”) fled Spain to Argentina in 2004, but was placed under surveillance by the authorities in a joint international operation.

The investigation also resulted in a number of other arrests, including that of an Eastern European computer engineer who claimed that Rodríguez was the mastermind behind the gang.

As banks and other organizations concerned by increasingly targeted phishing attacks move towards introducing stronger multi-factor authentication methods, it is only a matter of time before the phishers respond. Already, many banks across Europe now employ some form of two-factor authentication – which requires more than a username and password (the first factor) to authenticate to a website – they also require some form of one-time password (the second factor). In some cases these two-factor systems are implemented using single-use passwords provided in advance, for example in a scratch-off sheet along with the customers' monthly statement.

A recent phishing attack against Nordea, a well-known Scandinavian bank utilizing this type of system, also included the email address of the phishing target in the URL of the phishing site. Anyone clicking on such a link will inevitably provide the criminals with additional information with which to fine-tune their future activities. It was first thought that banks switching over to two-factor authentication schemes would be afforded some breathing space as the criminals continued to focus on the banks that used traditional methods for security. However, it seems that by phishing for a user's one-time password in this way, the criminals are able to collect these codes in the same fashion.

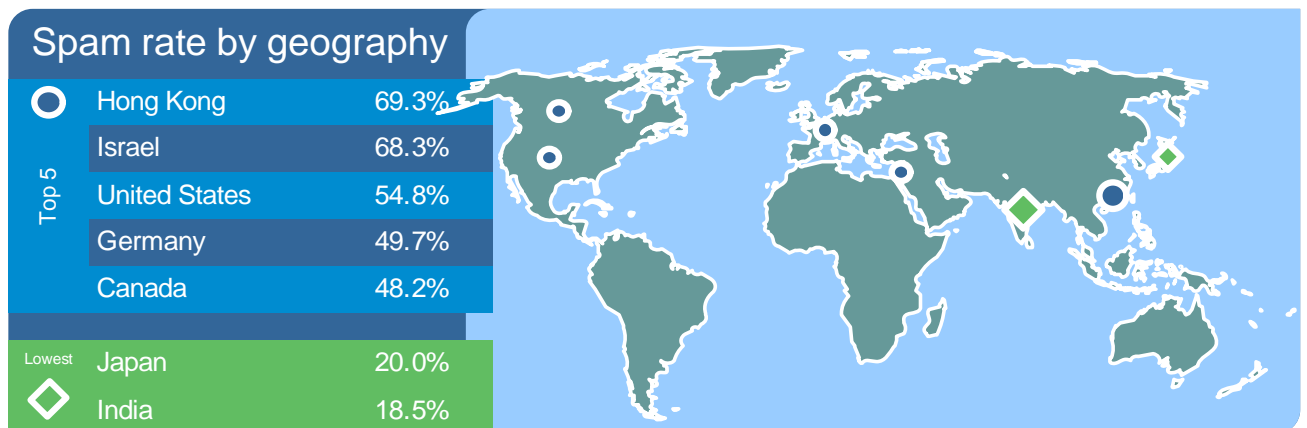
Perhaps more security may be afforded by another kind of two-factor system – a hardware device that generates single-use codes “on-the-fly,” for example like the key-ring sized device being introduced in May by HSBC for its 180,000 UK business internet banking customers. These numbers, even if collected, are only valid for a very short period of time and a new code is created ever minute, for example. HSBC is not the first UK bank to travel this path, as last year LloydsTSB, another high-street bank, began trialing similar devices with a number of its customers.

Last year, the U.S. Federal Financial Institutions Examinations Council (FFIEC) set a deadline at the end of 2006 for the U.S. banking industry to introduce multi-factor authentication for all internet transactions. In the UK no such mandate exists at the moment, although the banking industry is working closely with the Association for Payment Clearing Services (APACS) to agree a standard across the industry for two-factor authentication, possibly using a card-reader device.

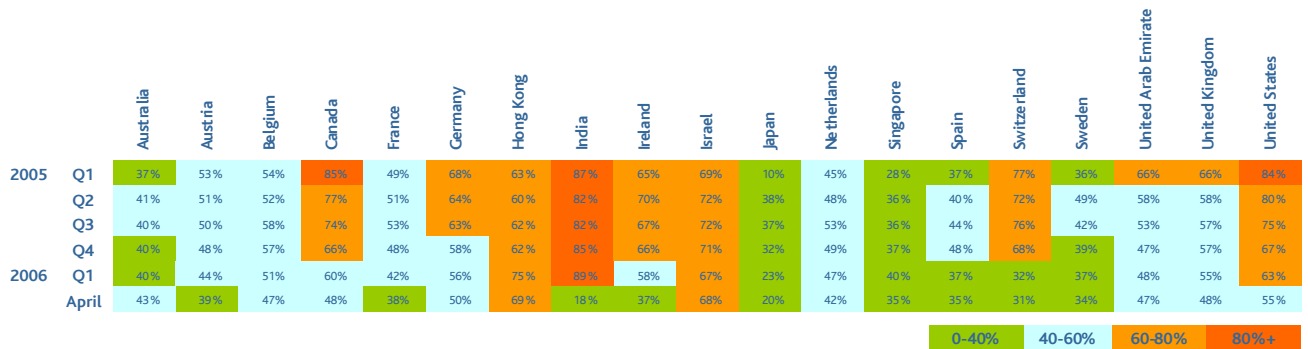
With more than £23 million lost in the UK through phishing in the last year and an estimated \$1 billion in the U.S., it will be interesting to see whether phishing attacks against banks employing tighter security controls will diminish in the coming months, or if in time there will be a step-change in the use of more sophisticated phishing trojans able to hijack online banking services after the user has completed the authentication process.

### Geographical Breakdown: Based on Targeted Countries

**April:** By analyzing the geographical dispersal of email traffic where possible, MessageLabs compiles data that shows the impact and vulnerability rates of spam and viruses specific to geographies. The charts below reflect impact and ratios for April 2006:



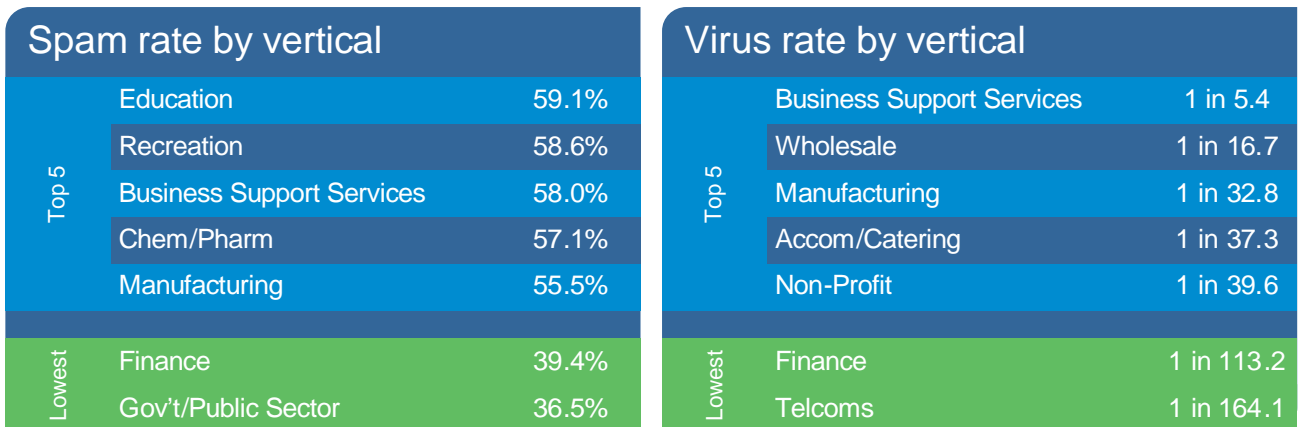




When this profile has been observed previously, MessageLabs has subsequently noted an increase in spam designed to be more difficult to detect using traditional methods. This is perhaps not unexpected, since many of the IP addresses in the region that have been compromised in recent months are well known, and have therefore been devalued for use by spammers who are likely to be seeking new ways to bypass spam filters.

### Vertical Industry Breakdown

**April:** By analyzing the market distribution of email traffic where possible, MessageLabs compiles data that shows the impact and vulnerability rates of spam and viruses specific to major industry sectors. The charts below reflect impacts and ratios for April 2006:



Again, Business Support Services was the main vertical victim in April, with 1 in 5.4 emails (18.4% of email traffic) heading for this vertical harboring a virus or some form of malware. This represents a 4.9% increase from 1 in 7.4 (13.5%) on the previous month, the largest shift for any vertical.

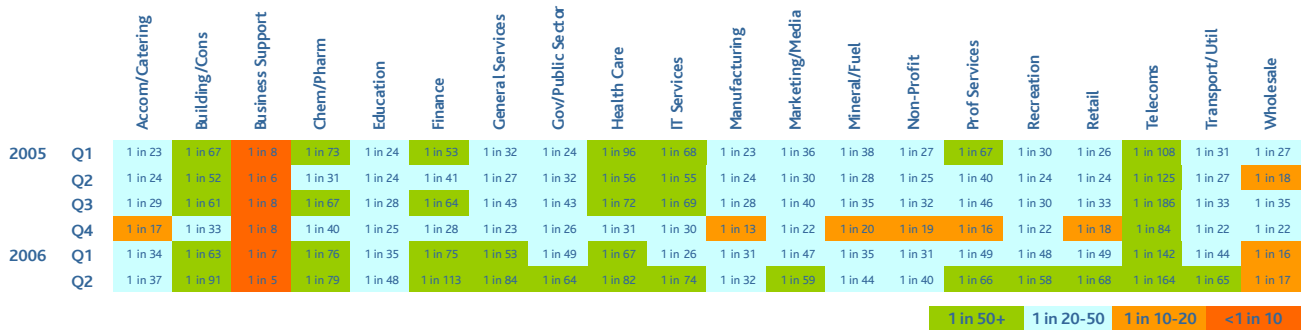
This vertical also witnessed the greatest increase across all sectors in terms of spam compared with last month. In March, MessageLabs intercepted 43.1% (1 in 2.32) of email traffic identified as spam heading for clients in the Business Support Services sector. In April, this increased by 14.9% to 58% (1 in 1.72).

Spam interceptions for the Education sector also increased this month by 4.3% from 54.9% (1 in 1.82) in March to 59.1% (1 in 1.69) this month, although virus interceptions fell by 1% from 1 in 32.9 (3%) in March to 1 in 48.5 (2.1%) in April.

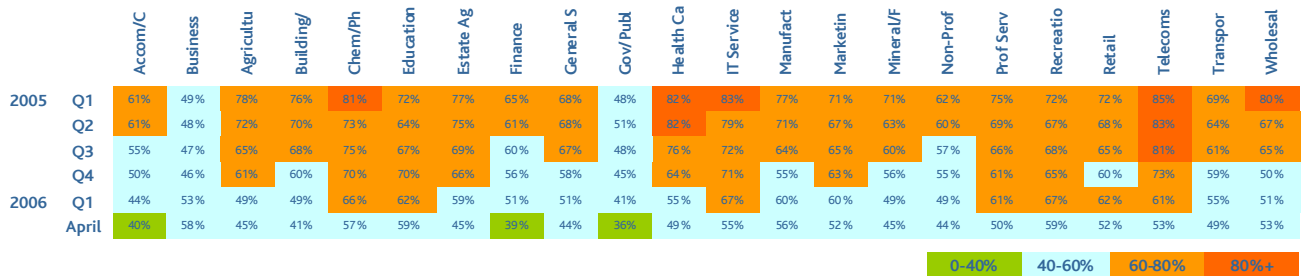
Whilst spam destined for the Telecoms sector rose by 2.6% from 50.2% (1 in 1.99) in March to 52.8% (1 in 1.90) the ratio of healthy to unhealthy emails intercepted during the same period fell further this month by 0.1% from 1 in 143.4 (0.7%) in March, to 1 in 164.1 (0.6%). With the keen adoption of VoIP and other innovative communication tools which hackers are taking note of, it's not certain how much longer will this sector will be able to maintain its enviable position.

**Quarterly Review:** The Business Support Services sector continues to be plagued by spam and virus traffic (as can be seen from the charts below). This vertical includes businesses that provide office administration and support functions as well as human resourcing and recruitment agencies.

Recruitment agencies in particular often suffer collateral damage from large outbreaks, since their email addresses regularly appear in people's address books, which may also be connected through online social networking tools.



The vertical with the greatest proportion of spam interceptions in Q1 was the IT Services sector, which includes IT support, outsourcing, technology consulting and IT training companies.



Although spam across all verticals in Q1 has fallen when compared with the same period last year (with the notable exception of Business Support Services), little comfort should come from this as global spending on anti-spam solutions is expected to exceed \$1.7 billion by 2008, according to IDC in Q1 2005. Yet despite this apparent investment, spam continues to be a problem across all verticals

### Traffic Management (Protocol Level)

Traffic Management continues to reduce the overall message volume through techniques operating at the protocol level. Unwanted senders are identified and connections to the mail server are slowed down using features embedded in the TCP protocol. Incoming volumes of known spam are significantly slowed, while ensuring legitimate email is expedited.

### Connection Management

Connection Management is particularly effective in stopping directory harvest, brute force and email denial of service attacks, where unwanted senders send high volumes of messages to force spam into an organization or disrupt business communications.

Connection Management works at the SMTP level using techniques that verify legitimate connections to the mail server, and is comprised of the following:

**SMTP Validation:** Identifies unwanted email originating from known spam and virus sending sources, where the source can unequivocally be identified as an open proxy or a botnet, and rejects the connection accordingly. In April, on average 5.6% of inbound messages were intercepted from botnets and other known malicious sources and rejected as a

consequence.

*Registered User Address Validation:* Reduces the overall volume of emails for registered domains, by discarding connections for which the recipients are identified as invalid or non-existent. In April, on average 9.4% of recipient addresses were identified as invalid; these were attempted directory attacks upon domains that were therefore prevented.

The table below details the current impact of connection management techniques on unwanted email volume being measured by MessageLabs Intelligence. Without these additional multiple layers of defense, spam traffic destined for MessageLabs clients in April would otherwise account for an average of 82.9% of global email traffic.

Region	SMTP Validation (botnet sources)	User Validation (directory attacks)
USA	6.0%	9.5%
UK	4.9%	8.9%
Europe	5.3%	10.1%
Asia Pacific	7.3%	8.4%
<b>Worldwide</b>	<b>5.6%</b>	<b>9.4%</b>

**MessageLabs** is the world's leading provider of email security and management services with more than 13,000 clients.

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 its control towers around the world.

For further information on MessageLabs Intelligence, please visit [www.messagelabs.com/intelligence](http://www.messagelabs.com/intelligence) and register to receive regular alerts and reports.

*NB: All figures mentioned in this report were correct at the time of going to press.*