MessageLabs Intelligence: October 2006
"Do you want spam with that spam?"

Introduction

Welcome to the October edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for October 2006, to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

Top line results of this report include:

Spam – 72.9% in October (an increase of 8.5% since September)
Viruses – One in 100.3 emails in October contained malware (a decrease of 0.12% since September)
Phishing – One in 190 emails comprised a phishing attack (a decrease of 0.06% since September)

October marks the beginning of the spam season this year in the run up to the holiday period, with MessageLabs seeing a sharp increase in levels this month, especially in the past few weeks. As predicted in the September/Q3 MessageLabs Intelligence report, spam is not going away. This increase is largely attributed to the huge rise in botnet activity over the past few weeks.

There are two contributing factors compounding this issue, and it is as yet unclear as to whether there is any link between them. The first culprit is the aggressive level of activity around one particular trojan dropper called Warezov. Tens of thousands of copies of each variant are dispatched in numerous batches, where each batch is subtly different from the previous ones. Even a few bytes changed in the code will allow the trojan to pass undetected through traditional anti-virus protection. Being a dropper it is uncertain as to what the trojan is being used for, however it seems clear that there is a connection with the huge rise in spam levels around the world.
The second driver of increased spam is another trojan, dubbed "SpamThru" which is responsible for a great deal of the botnet activity behind increased levels of spam this month. Analysis of SpamThru shows that the SpamThru makers are releasing new strains at regular intervals in order to confound traditional anti-virus signature detection. Using the "spam cannon" technique mentioned in previous reports, SpamThru utilizes a template for each spam it sends and by combining it with a list of email addresses, each zombie is then able to pump out millions of spam emails.

Although designed to turn the infected computer into a spam-sending zombie, SpamThru employs an interesting device to circumvent the closure of the command-and-control channel. Usually, the control channel (or mother-ship) is located on an Internet Relay Chat (IRC) server under the control of the botnet master, and if this channel is disrupted, he/she may lose control of the entire botnet.

However, rather than relying upon a central mother-ship for the control channel, each SpamThru zombie is able to learn about the other zombies in the botnet and relay that information when requested. Command and control is still centralized with SpamThru but should the control channel become disrupted, the botnet controller can regain control of the botnet by having access to just a single zombie machine on the botnet.

SpamThru also attempts to neutralize anti-virus software by corrupting the local "hosts" file, inserting dummy addresses to override genuine anti-virus update URLs. SpamThru also downloads an illegal copy of Kaspersky Anti-Virus onto the infected computer, scanning the PC for viruses, whilst ensuring that it bypasses its own components. Interestingly, any

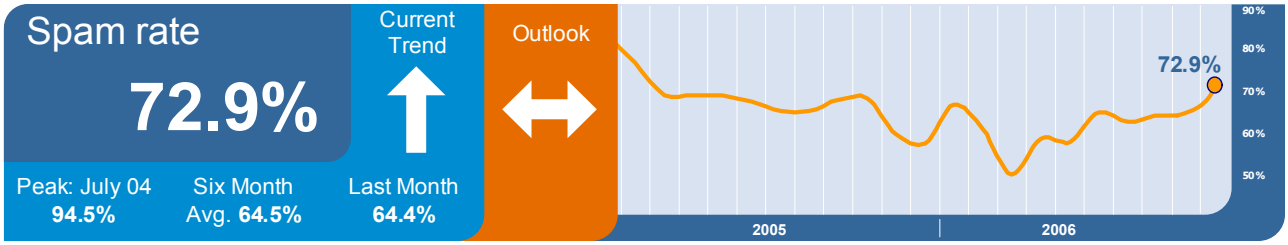
other malware found on the system is removed the next time Windows reboots.

With stagnant spam levels being the norm in recent months and significant increases being a distant memory, spam appears to be having a resurgence and will garner the attention, recently owned by viruses and phishing, through aggressive new techniques.

Global Trends & Content Analysis

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

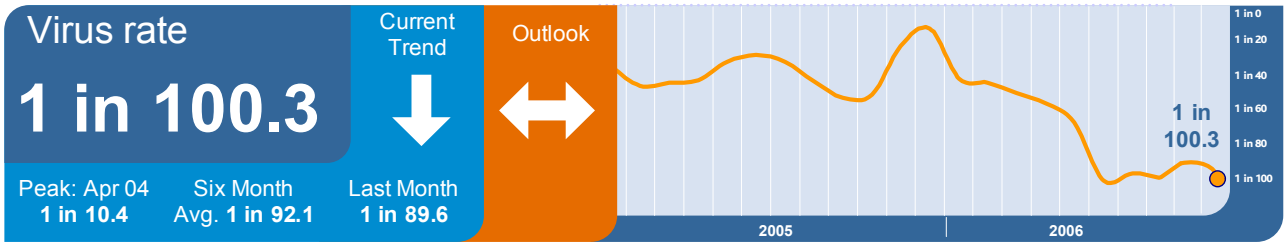
Skeptic™ Anti-Spam Protection: In October 2006, the global ratio of spam in email traffic from new and unknown bad sources, for which the recipient addresses were deemed valid, was 72.9% (1 in 1.37 emails), an increase of 8.5% on the previous month. This is the sharpest rise in spam levels since January 2006, when an increase of 9.2% was observed.



The figure of 72.9% is actually lower than the “true” spam figure since MessageLabs deployed additional layers of defense at its network perimeter in early 2005, known as Traffic Management. This enables MessageLabs to control the amount of bandwidth that is given to absolutely known bad-sources of spam, and then to throttle those connections, slowing them down to a crawl so that to the spammer, they appear to be talking to a very slow modem.

This in turn makes it incredibly painful for spammers attempting to send their spam to MessageLabs clients as it is effectively pushing back the spam to their networks by slowing-down their ability to send lots of spam. Consequently, many such connections eventually “time-out” or move on to softer targets. If we look at the amount of spam hitting MessageLabs honey-pots, which are unprotected by comparison, this figure would be much closer to 88.7%. For further information, please refer to the section on Traffic Management later in this report.

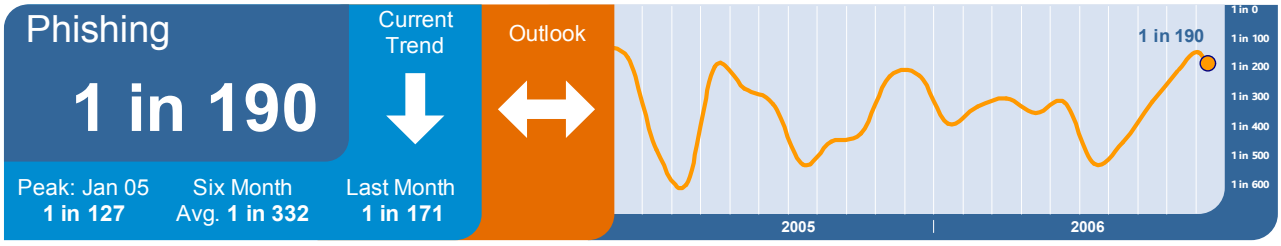
Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic from new and previously unknown bad sources destined for valid recipients, was 1 in 100.3 emails (1.0%) in October, a decrease of 0.12% since last month.



Although virus levels have seemingly fallen, this figure contradicts the true picture of the latest virus patterns. October witnessed a great deal of activity where dozens of copies of the Warezov dropper were mass-mailed in batches, where each batch of executables was modified in an attempt to avoid signature based detection. This resulted in a continuous burst of new viruses unable to be detected by traditional means, continually extending the window of vulnerability between release and protection. The net effect was an explosion in the number of spam-sending zombies on the internet, further aggravating an already acute spam problem.

Phishing: October showed a slight decrease of 0.06% in the proportion of phishing attacks compared with the previous month. One in 190 (0.53%) emails comprised some form of phishing attack.

When judged as a proportion of all email-borne threats such as viruses and trojans, the number of phishing emails has stabilized after a significant increase of 30.7% the month before. 52.9% of all malicious emails intercepted by MessageLabs in October were phishing attacks, an increase of 0.5% on the previous month.



Phishing attacks continue to be targeted mostly at those banks that have not currently deployed any two-factor authentication security measures. Banks that have deployed this technology are still being subjected to attacks, but on a much lesser scale.

October also saw the release of Microsoft Internet Explorer 7.0 and Mozilla Firefox 2.0, both of which include additional anti-phishing countermeasures, so it remains to be seen as to what effect this will have on the nature of phishing attacks over the coming months.

Skeptic™ Web Security Services Version 2.0: In July 2006, MessageLabs launched version 2.0 of its Web Security Services, built on MessageLabs proprietary technology. Web Security Services using Skeptic paves the way for the introduction of MessageLabs Converged Threat Analysis™, taking the very latest threat and reputation information from other protocols, such as email, and applying that knowledge to web traffic.

It can be seen from the chart below that the most common trigger for policy-based filtering, applied by MessageLabs for its business clients, is Proxies & Translators (38.4%). This category includes remote proxies for anonymous surfing, search engine caches that circumvent filtering and web-based translation sites that circumvent filtering, for example, Babelfish and Proxify.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Proxies & Translators	38.4%	Backdoor.Win32.Hupigon.clt	38.0%	Adware-SaveNow	55.1%
Advertisements & Popups	31.1%	Trojan.Win32.Diamin.ez	27.9%	Adware-ISTbar.b	23.1%
Spyware	10.8%	Trojan-Clicker.HTML.Agent.a	12.6%	Adware-abetterintrnt.gen.a	21.5%
Adult/Sexually Explicit	4.4%	VBS/Psyme	3.3%	Adware-ZangoSA	0.4%
Streaming Media	2.7%	Phish-BankFraud.eml.b	2.0%		
Chat	1.8%	Downloader-ABJ	1.4%		
Blogs & Forums	1.6%	Suspicious IFrame-c	1.2%		
Unclassified	1.5%	W32/Bagle.gen	1.0%		
Gambling	1.1%	Trojan-Downloader.HTML.Agent.ae	1.0%		
Downloads	1.0%	JS/Wonka	0.9%		

The “Unclassified” category identifies new and previously uncategorized sites that may potentially need to be prohibited. The Unclassified category affords more confidence when defining new rules, which means that newly detected malicious sites may be handled more appropriately until categorized, thereby safeguarding against sites which appear and disappear within a 24 to 48 hour timeframe; such sites may be used for disreputable purposes, such as hosting phishing and spam sites, information stealing trojans and other fraudulent activities.

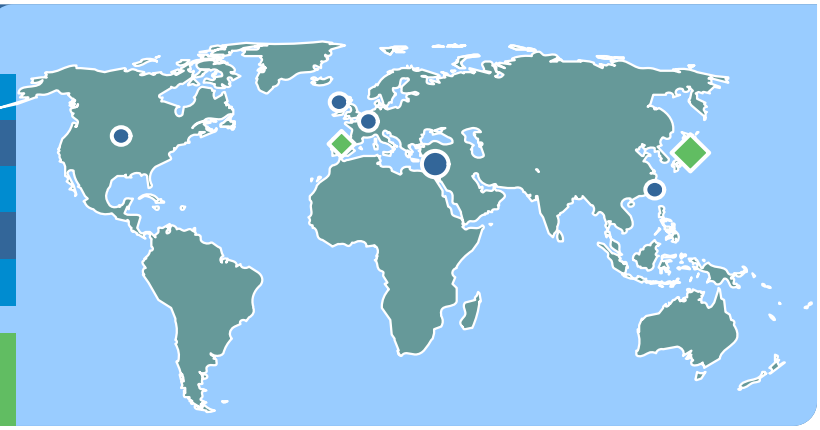
Analysis of web security activity also shows that 94.4% of interceptions occur as the result of a rule triggered by a policy which has been implemented by a system administrator. However, 5.6% of interceptions are also the result of malware or potentially unwanted programs, including adware and spyware that was detected heuristically by Skeptic.

Geographical Breakdown: Based on Targeted Countries

Monthly Analysis: 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 October 2006.

Spam rate by geography

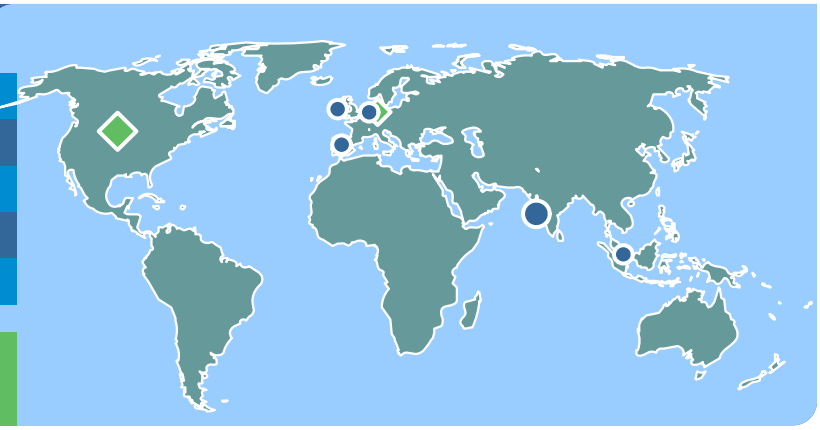
Top 5	Israel	84.4%
	United States	72.2%
	Ireland	71.1%
	Hong Kong	69.6%
	Germany	66.3%
Lowest	Spain	42.9%
	Japan	35.7%



In October, the top-5 countries in receipt of the majority of spam are largely unchanged from the previous month, however, there have been some position fluctuations. Israel retained the top-spot, with an increase of 9.1%. The US moved into second place with a rise of 11.5%, whilst Ireland slipped into third place with a rise of 6.9%. Further increases were borne in Hong Kong and Germany, by 9.2% and 8.7% respectively. Even the countries at the foot of the table witnessed significant increases this month, Spain by 6.8% and Japan increasing by 10.7%. The largest rise was in India, which had the lowest spam levels in September. In October, spam levels jumped by a massive 21.0% from 28.3% to 49.3%.

Virus rate by geography

Top 5	India	1 in 16.0
	Ireland	1 in 24.3
	Germany	1 in 36.1
	Singapore	1 in 49.8
	Spain	1 in 52.6
Lowest	Netherlands	1 in 134.0
	United States	1 in 135.7



India remains the hardest hit country in terms of virus activity, where 6.24% (1 in 16) of inbound email traffic contains a virus, trojan or other form of malware. This represents a fall of 1.47% since September. Virus levels in Ireland however increased by 0.30% to 4.12% (1 in 24.3) of email traffic. Virus activity in the US fell by 0.36% to 0.74% (1 in 135.7) of emails, pushing it to the bottom of the table this month. Although this may seem a rather enviable position, the ratio of email borne virus traffic is still uncomfortably high regardless. Australia elevated from being near the foot of the table in the previous month, to a mid-table ranking in October; increasing by 0.38% to 1.19% (1 in 84.1) of email traffic.

Vertical Industry Breakdown

Monthly Analysis: 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 October 2006.

Spam rate by vertical

Top 5	Education	76.2%
	Manufacturing	73.6%
	IT Services	72.8%
	Telecoms	70.1%
	Retail	68.1%
Lowest	Finance	56.2%
	Gov/Public Sector	48.8%

Virus rate by vertical

Top 5	Business Support Services	1 in 30.3
	Education	1 in 44.8
	Wholesale	1 in 48.2
	Gov/Public Sector	1 in 73.4
	Non-Profit	1 in 75.2
Lowest	Health Care	1 in 153.3
	Telecoms	1 in 232.9

Education, Manufacturing and Telecoms remain in the top-5 verticals listing, all achieving 10.0% or higher increases this month. These sectors are joined by IT Services, which levels rose the most significantly of all sectors, by 18.2% and rose from 10th position in September, and Retail with an 10.8% rise in levels. Overall, spam levels across all sectors have increased in October, with Recreation having the lowest increase of 1.9%.

The Public Sector has climbed from 8th position in September to push Manufacturing out of the top-5 industries most affected by virus attacks. This is in spite of a drop of 0.16% to 1.36% (1 in 73.4) of inbound email traffic.

Virus traffic destined for Business Support Services fell by 3.69% to 3.30% (1 in 30.3) of emails, the most significant decrease of all sectors. Overall, virus traffic fell across almost all industry sectors in October, only with Building/ Construction and Recreation receiving minor increases.

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.

In October, MessageLabs processed over 2.35 billion SMTP connections per day, of which 92.2% of these connections were throttled back as a result of traffic management protocol controls for traffic that was unequivocally malicious or unwanted.

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 October, an average of 4.7% 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 October, an average of 11.4% of recipient addresses were identified as invalid; these were attempted directory attacks upon domains that were therefore prevented.

Summary

The table below details the current impact of traffic and 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 October would otherwise account for around 88.7% of global email traffic, an increase of 6.6% on the previous month.

Region	Traffic Management *(protocol control)*	SMTP Validation *(behaviour analysis)*	User Validation *(directory attacks)*
USA	94.20%	4.10%	12.00%
UK	90.00%	5.60%	11.40%
Europe	88.10%	4.90%	11.80%
Asia Pacific	80.30%	2.90%	5.40%
Worldwide	**92.20%**	**4.70%**	**11.40%**

Effects of Traffic Management Techniques

MessageLabs is a leading provider of integrated messaging and web security services, with over 15,000 clients ranging from small business to the Fortune 500 located in more than 80 countries. MessageLabs provides a range of managed security services to protect, control, encrypt and archive communications across Email, Web and Instant Messaging.

These services are delivered by MessageLabs globally distributed infrastructure and supported 24/7 by security experts. This provides a convenient and cost-effective solution for managing and reducing risk and providing certainty in the exchange of business information. For more information, please visit www.messagelabs.com.

For further information on MessageLabs Intelligence, please visit 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.

Appendices

Appendix I: Spam Rate by Geography (October 2006)

	October	September	Change
Australia	60.30%	47.70%	12.60%
Austria	61.30%	52.10%	9.20%
Belgium	54.30%	52.70%	1.60%
Canada	65.90%	51.40%	14.50%
France	58.80%	51.40%	7.40%
Germany	66.30%	57.60%	8.70%
Hong Kong	69.60%	60.40%	9.20%
India	49.30%	28.30%	21.00%
Ireland	71.10%	64.20%	6.90%
Israel	84.40%	73.60%	10.80%
Italy	60.90%	54.00%	6.90%
Japan	35.70%	25.00%	10.70%
Netherlands	59.10%	48.00%	11.10%
Singapore	65.30%	55.40%	9.90%
Spain	42.90%	36.10%	6.80%
Sweden	52.40%	39.20%	13.20%
Switzerland	52.70%	42.50%	10.20%
United Arab Emirates	63.50%	53.60%	9.90%
United Kingdom	61.40%	51.40%	10.00%
United States	72.20%	60.70%	11.50%

Appendix II: Virus Rate by Geography (October 2006)

	October	September	Change
Australia	1.19%	0.81%	0.38%
Austria	0.89%	0.97%	-0.08%
Belgium	0.75%	0.52%	0.23%
Canada	0.76%	0.96%	-0.20%
France	1.47%	1.98%	-0.51%
Germany	2.77%	3.27%	-0.50%
Hong Kong	1.85%	2.28%	-0.43%
India	6.24%	7.71%	-1.47%
Ireland	4.12%	3.82%	0.30%
Israel	0.94%	1.01%	-0.07%
Italy	1.00%	1.18%	-0.18%
Japan	1.25%	1.38%	-0.13%
Netherlands	0.75%	0.89%	-0.14%
Singapore	2.01%	2.20%	-0.19%
Spain	1.90%	3.14%	-1.24%
Sweden	1.01%	1.12%	-0.11%
Switzerland	1.26%	1.47%	-0.21%
United Arab Emirates	1.70%	3.24%	-1.54%
United Kingdom	1.29%	1.19%	0.10%
United States	0.74%	1.10%	-0.36%

Appendix III: Spam Rate by Vertical (October 2006)

	October	September	Change
Accom/Catering	60.50%	52.80%	7.70%
Building/Cons	57.70%	49.50%	8.20%
Chem/Pharm	65.60%	57.60%	8.00%
Education	76.20%	62.90%	13.30%
Estate Agents	60.00%	54.20%	5.80%
Finance	56.20%	46.70%	9.50%
General Services	57.20%	53.50%	3.70%
Gov/Public Sector	48.80%	40.70%	8.10%
Health Care	66.40%	56.80%	9.60%
IT Services	72.80%	54.60%	18.20%
Manufacturing	73.60%	62.30%	11.30%
Marketing/Media	67.30%	56.50%	10.80%
Mineral/Fuel	61.30%	52.60%	8.70%
Non-Profit	63.90%	54.80%	9.10%
Prof Services	66.00%	56.10%	9.90%
Recreation	60.80%	58.90%	1.90%
Retail	68.10%	57.30%	10.80%
Telecoms	70.10%	60.10%	10.00%
Transport/Util	68.10%	57.70%	10.40%
Wholesale	66.30%	56.70%	9.60%

Appendix IV: Virus Rate by Vertical (October 2006)

	October	September	Change
Accom/Catering	1.31%	1.53%	-0.22%
Building/Cons	1.04%	0.99%	0.05%
Business Support Services	3.30%	6.99%	-3.69%
Chem/Pharm	0.79%	1.01%	-0.22%
Education	2.23%	2.39%	-0.16%
Finance	1.18%	1.01%	0.17%
General Services	1.08%	1.17%	-0.09%
Gov/Public Sector	1.36%	1.52%	-0.16%
Health Care	0.65%	0.75%	-0.10%
IT Services	0.66%	0.71%	-0.05%
Manufacturing	1.18%	1.55%	-0.37%
Marketing/Media	1.01%	1.14%	-0.13%
Mineral/Fuel	1.18%	1.31%	-0.13%
Non-Profit	1.33%	1.54%	-0.21%
Prof Services	0.89%	0.92%	-0.03%
Recreation	1.03%	1.02%	0.01%
Retail	0.92%	1.07%	-0.15%
Telecoms	0.43%	0.54%	-0.11%
Transport/Util	1.01%	1.20%	-0.19%
Wholesale	2.07%	2.78%	-0.71%