MESSAGELABS INTELLIGENCE APRIL 2010

Survival of the Fittest: Selfish Botnets Dominate the Spam Landscape as Rustock Becomes the Largest Botnet; Linux Takes a Share of Spam from Windows

Welcome to the April edition of the MessageLabs Intelligence monthly report. This report provides the latest threat trends for April 2010 to keep you informed regarding the ongoing fight against viruses, spam and other unwelcome content.

REPORT HIGHLIGHTS

- Spam – 89.9% in April (a decrease of 0.8 percentage points since March)
- Viruses – One in 340.7 emails in April contained malware (an increase of 0.01 percentage points since March)
- Phishing – One in 455.2 emails comprised a phishing attack (an increase of 0.03 percentage points since March)
- Malicious websites – 1,675 websites blocked per day (a decrease of 12.7% since March)
- 33.6% of all malicious domains blocked were new in April (a decrease of 6.3 percentage points since March)
- 10.9% of all web-based malware blocked was new in April (a decrease of 4.0 percentage points since March)
- A review of the world's largest spam-sending botnets
- Rustock becomes the largest and most active botnet
- The selfish botnets - Survival of the fittest in the wake of McColo
- Fingerprinting spam-sending botnets – Identifying the operating systems behind the botnets
- Ten Year Anniversary of the LoveBug virus

REPORT ANALYSIS

Spam-sending botnets: An in-depth review of robot networks for 2010

Rustock is now not only the loudest, but also the biggest botnet around.

Rustock has, on average, reduced the output of individual bots by 65%. However, the number of active bots in the botnet has increased by around 300% to between 1.6 and 2.4 million bots, which more than compensates for the decreased output per bot. This now makes Rustock the biggest botnet both in terms of the amount of spam it sends, and also the number of zombie machines under its control (taking the top spot away from Cutwail).

The increased number of bots has also changed the geographical distribution of the botnet. Previously Brazil was the top infected country by a large margin, but now the top three Rustock-infected countries are India, USA, and Brazil.

Cutwail on the other hand, has been greatly reduced in size. At its height, around the end of May 2009, it had almost 2 million bots under its control. It was also pushing these bots to send out over 250 spam messages each per minute, and this made it the source of almost half of all global spam.

In the most recent analysis however, Cutwail's size has dropped to around 600,000 bots, and the output of each bot is now only around 40 spam emails per minute. This means that although it is still the third biggest botnet (behind Rustock and Grum) in terms of the number of bots it controls, it now only outputs 4% of global spam.

botnet	% of spam	spam/day	spam/min	spam/bot/ min	estimated botnet size	Country of Infection
rustock	32.8%	43,417,898,965	30,151,319	96	1600k to 2400k	India (8%), USA (7%), Brazil (6%)
grum	23.9%	31,586,177,785	21,934,846	146	800k to 1200k	Russia (13%), India (10%), RepKorea (7%)
mega-d	17.7%	23,359,048,273	16,221,561	428	190k to 290k	Russia (35%), Ukraine (18%), Kazakhstan (7%)
bagle	4.3%	5,682,582,027	3,946,238	131	150k to 230k	USA (8%), Netherlands (7%), Colombia(6%)
cutwail	4.2%	5,594,372,460	3,884,981	41	490k to 730k	Vietnam (17%), RepKorea (15%), Brazil (11%)
bobax	3.0%	3,933,960,384	2,731,917	232	60k to 80k	India (18%), Brazil (7%), Russia (6%)
lethic	1.5%	1,992,469,767	1,383,660	33	210k to 310k	Netherlands (16%), UK (7%), Israel (6%)
maazben	0.4%	496,891,816	345,064	42	40k to 60k	Brazil (43%), Vietnam (9%), India (7%)
xarvester	0.1%	146,731,371	101,897	75	8k to 12k	Brazil (16%), USA (10%), Poland (8%)
gheg	0.2%	234,343,492	162,739	38	24k to 36k	Spain (10%), Brazil (9%), USA (8%)
Unclassified Botnets	3.7%	4,930,668,112	3,424,075	87	140k to 200k	
Other, smaller botnets	0.2%	229,538,426	159,402	22	24k to 36k	
Total BotnetSpam	**92.0%**	**121,604,682,877**	**84,447,696**	**114**	**3700k to 5600k**	**Russia (9%), India (7%), USA (6%)**
Non-botnet spam	**8.0%**	**7,006,676,396**	**4,865,747**			
Grand Total	**100.0%**	**128,611,359,273**	**89,313,444**			10-17 MAR 2010

Figure 1 – Top spam-sending botnets in 2010

Cutwail was affected by the closure of Real Host, a Latvian ISP, in August 2009 and it is likely that it lost the ability to update some of its bots; consequently its numbers diminished gradually without being able to recover. Other botnets such as Rustock may be undercutting the market with greater capacity and lower operational costs. As a result, Cutwail has lost significant volumes of business from spammers. As well as spam, Cutwail has also been used to distribute malware such as the Bredolab trojan, perhaps an indication that it has sought to diversify its business model over the past year.

The botnet Mega-D has been around since January 2008, but after November 2008, it suffered a number of setbacks: First, in November 2008 when the McColo ISP was taken down Mega-D was almost completely taken out. In November 2009, community action led by researchers at FireEye[1] attempted to take it down again, and for a while seemed to have succeeded. In both cases Mega-D managed to recover, and it is currently the third most active botnet, responsible for 18% of all global spam.

[1] *http://www.symantec.com/connect/blogs/mega-d-aka-ozdok-crippled*

Despite having not nearly as many bots as the top two (Mega-D currently controls approximately 240,000 bots), it works these bots very hard, pushing them to output around 430 spam emails per bot per minute. This makes Mega-D currently the hardest working botnet overall. Previously, Mega-D's bots were spread around the world, the highest proportions in Vietnam, Brazil, and India. Now though, Mega-D seems to be originating almost entirely within Eastern Europe, with the top three infected countries being Russia, Ukraine, and Kazakhstan.

The output from Grum has been fairly consistent over the last five months, with each bot sending between 145 and 150 spam emails per minute. What is different though is that Grum has managed to greatly increase the number of bots under its control from approximately 700,000 to about 1 million. This increase has allowed Grum to become the second largest source of all global spam, second only to Rustock.

Historically, the countries with most botnet infected machines have been Brazil, USA, Republic of Korea, and Vietnam, but lately this has changed. Analysis shows that most of Grum and Mega-D's new bots are located in the Russian Federation. This combined with other botnets that have infections in the same area, means that the Russian Federation is now the country with the highest number of infected machines. As well as the Russian Federation, Rustock and Grum have managed to get a large number of new bots in India. Combined with other botnets like Bobax and Maazben, which also have a presence there, this has now made India the country with the second highest number of botnet infected machines in the world.

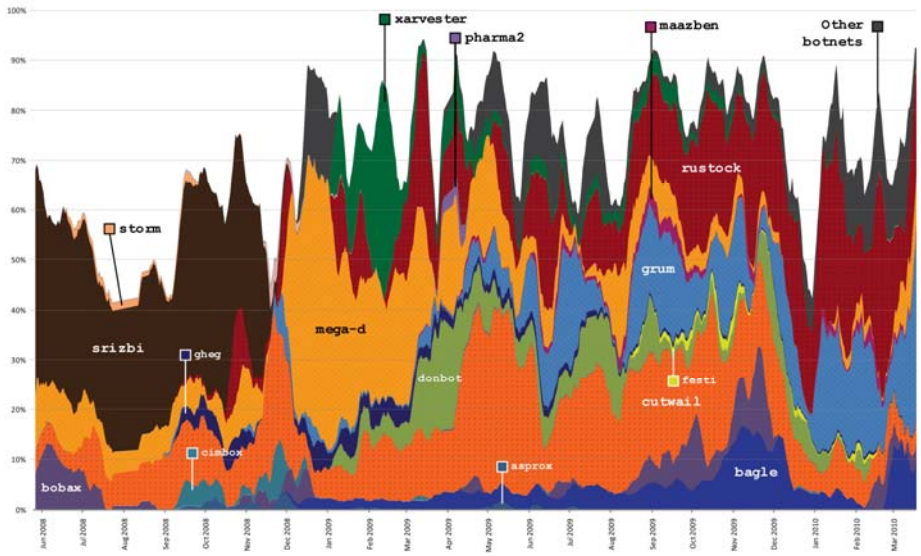


Figure 2 – Relative proportion of spam from botnets

The Selfish Botnets: Survival of the Fittest - A comparison of newer and more established botnets since the McColo shutdown of 2008

MessageLabs Intelligence looked at all the botnets we have seen over recent years, and separated them into two groups: Newer botnets, and more established botnets.

In figure 3, newer botnets are defined as any botnet first seen in 2009 or later – these are Donbot, Xarvester, Reposin, ZapChast, HelloGirl, Maazben, Banjor/Velrok, DarkMailer, Festi, MutandaX, Iflar, Lethic. More established botnets are defined as any botnet first seen before 2009 – these are Bagle, Dlena ZMailer, Fivetoone, Asprox, Gheg, Cimbot, Rustock, Cutwail, Storm, Srizbi, Mega-D, Bobax, Warezov/Stration, Grum. Other unnamed botnets are sources that we know are

botnets, but MessageLabs Intelligence has not yet established which ones and non-botnet is either spam that isn't from a botnet, but sent manually or through some other mechanism, or spam from an unidentified botnet.

After the demise of the McColo ISP in November 2008, which resulted in disruption to many heavyweight botnets, including the most notable Srizbi, there were large shifts in the relative dominance of well-established botnets. But also, out of the ashes, newer and more advanced botnets sprang onto the scene.

These include Donbot and Xarvester.

Despite being more advanced, with added protection against takedowns such as what happened with McColo, these new botnets arrived at a time when the level of awareness of botnets, and especially new botnets was extremely high. After McColo's success, the eyes of the global internet security community were on botnets and how to disrupt them.

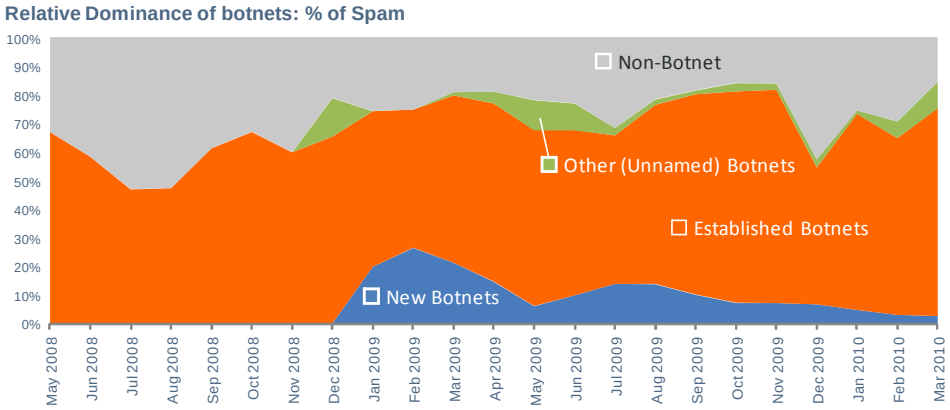


Figure 3 – Percentage of spam from botnets

At the beginning of 2009 MessageLabs Intelligence tracked 14 established botnets, including heavyweights Mega-D, Rustock, Cutwail, Bagle and Grum. However, since then, we have seen 12 more new botnets.

The graph in figure 3 above shows that the combined dominance of all of the new botnets has not been enough to overcome the dominance of the strong, established heavyweights. It is clearly very difficult for new botnets to grow and achieve the critical mass necessary to become harder to disrupt.

By critical mass we consider the following attributes: a consistent average for the number of bots, robust and well developed malware used to recruit new bots, multiple fail-over mechanisms, and an infrastructure that spans many different ISPs and networks around the world. A robust command and control mechanism should have no single points of failure. Much like Hydra, the water-beast of Greek mythology, these well-established botnets respond quickly to losing a head, by growing a new one.

In early 2009, two new botnets, Donbot and Xarvester, managed to build quite a reputation for themselves, before declining, while others were quickly disrupted and the more heavyweight botnets had a chance to re-group.

In late 2009 and early 2010, the more established botnets are again in charge, with Rustock, Grum, Mega-D, Bagle and Cutwail accounting for more than 80% of all spam, and 90% of all botnet spam.

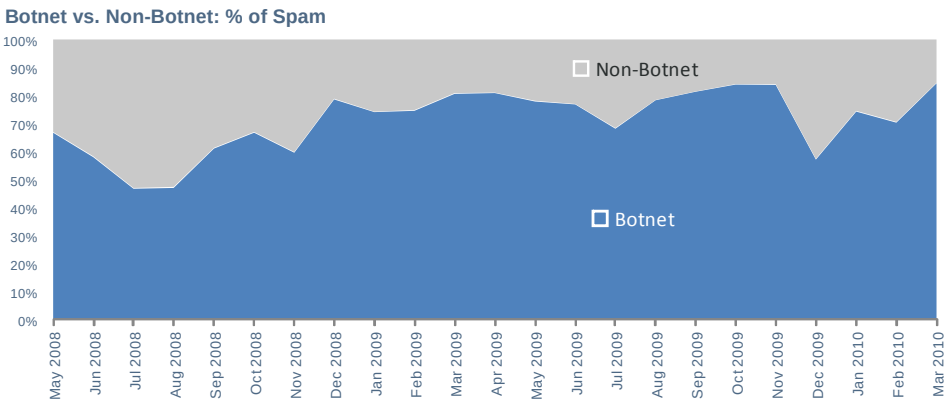


Figure 4 – Botnet vs. non-botnet spam

In figure 4, botnet spam is defined as spam that MessageLabs Intelligence knows comes from a botnet -- although we may not always know which one -- we have identified that a botnet is responsible. Non-botnet spam is either spam that we know isn't sent from a botnet, or spam that may be sent from a new botnet that we don't know about.

The average percentage of spam that is sent from botnets each month has not changed significantly over the last 12 months, but it is higher than in 2008. In 2008, this figure was about 60%, which meant that 60% of all spam was sent from a botnet. In 2009, this figure rose to 83.4% and by April 2010, the average percentage of spam sent from botnets was 84%.

Although this figure represents the monthly average, in a given day, the proportion of spam sent from botnets can surge to as high as 97% of spam. In 2008 the peak ratio of spam from botnets in a single day was 92% of spam.

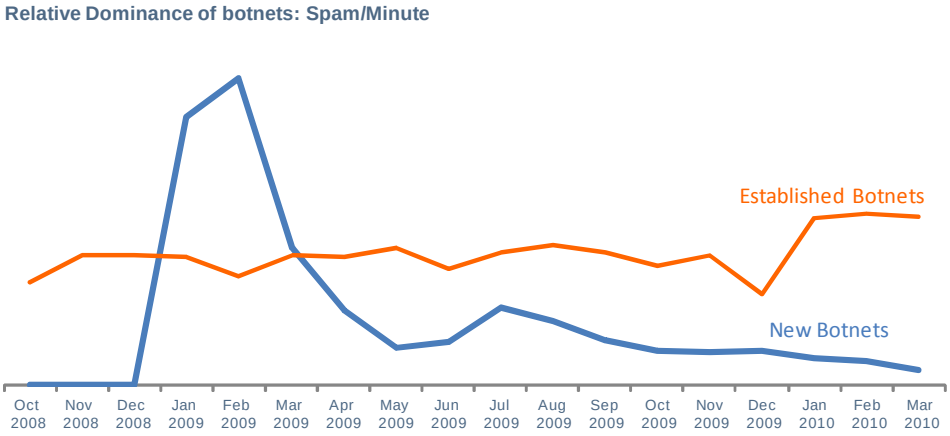


Figure 5 – Relative dominance of botnets: spam per minute

Another way to look at the activity of new botnets versus established botnets is to consider how much spam they send per minute, in other words how hard they are working.

This is a different approach to analyzing the percentage of spam, because it's not affected by what other botnets are doing at the same time. For example, if Rustock sends more spam, and the proportion of spam from Rustock increases, the percentage of spam from all the other botnets will appear to decrease slightly.

In figure 5 above, showing the level of output of new botnets versus established botnets, it can be seen that at the start of 2009, the average spam rate per minute from new botnets far exceeded the output from more established botnets. However,

as we saw earlier, the proportion of spam sent from new botnets never exceeded that from established botnets. This indicates that although these newer botnets may have been working very hard, there simply weren't enough of them to survive.

The average spam rate per minute from established botnets continued very steadily through 2008, 2009 and into 2010. Although some of those botnets were severely disrupted or destroyed by the closure of McColo, the average spam per minute from the surviving botnets remained steady.

For newer botnets, the output rate only exceeded that of the established botnets until March 2009, and this was almost entirely owed to Donbot and Xarvester. Moreover, they were eventually unable to sustain this high throughput rate for the remainder of 2009 and by April 2010 their average spam rate per minute was only a fraction of the average output of the more established botnets, like Rustock, Cutwail and Bagle.

Newer botnets: Spam rates per minute

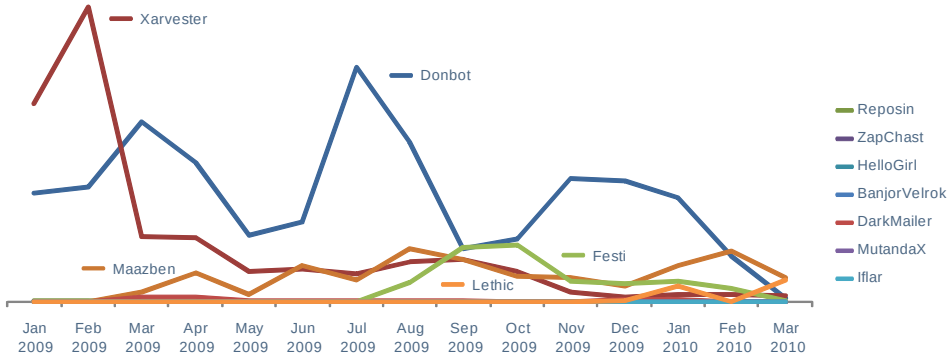


Figure 6 – Newer botnets: Spam rates per minute

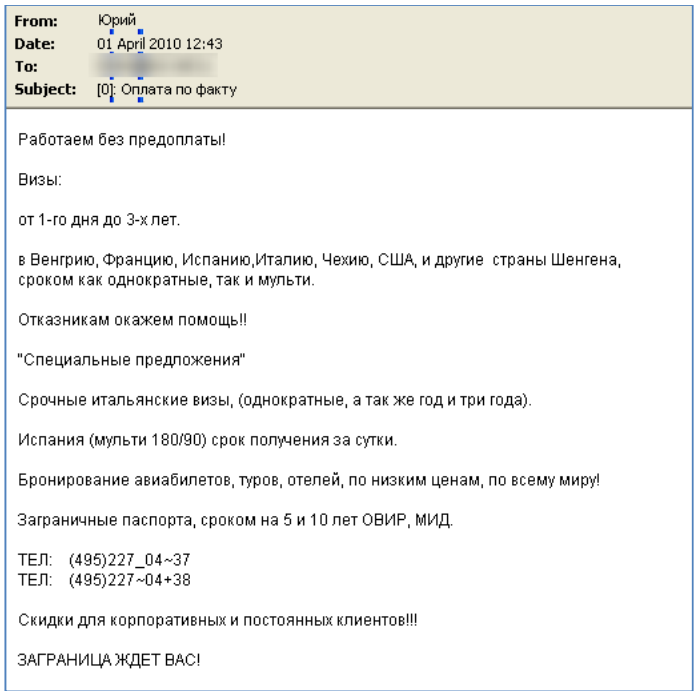
Figure 6, shows the average spam rate per minute for each month, for each of the new botnets since the beginning of 2009.

Of all the new botnets that appeared from the ashes of McColo, Donbot was the most successful. Donbot grew and continued to spam through 2009 and into 2010 with roughly three to four times the average spam rate per minute of any other new botnet. For a short time in March 2009, Donbot was the most active botnet, sending 17% of all spam, an estimated 17 billion spam messages every day. It was also responsible for a lot of spam during July and August 2009, and in November 2009 it was associated with several waves of spam campaigns containing links to social networking profiles and micro-blogging websites.

At its peak of activity during the first quarter of 2009, Donbot comprised an estimated 800,000 to 1.2 million bots, falling to an estimated 100,000-150,000 by the end of 2009. By April 2010 the estimated size of Donbot was about 10,000 bots.

At the start of 2010, Donbot had already faded from its earlier prominence, and by April 2010, Donbot may be all but gone. There is also the possibility that its bots have been upgraded with new Trojan malware that has not been identified as Donbot.

Just as Xarvester became a replacement for the Srizbi botnet after it was severely disrupted following the closure of McColo, it was also prolific at the beginning of 2009 and has quickly faded into relative obscurity by April 2010, with a very low output rate.



From: Юрий
Date: 01 April 2010 12:43
To: [redacted]
Subject: [0]: Оплата по факту

Работаем без предоплаты!

Визы:

от 1-го дня до 3-х лет.

в Венгрию, Францию, Испанию,Италию, Чехию, США, и другие страны Шенгена, сроком как однократные, так и мульти.

Отказникам окажем помощь!!

"Специальные предложения"

Срочные итальянские визы, (однократные, а так же год и три года).

Испания (мульти 180/90) срок получения за сутки.

Бронирование авиабилетов, туров, отелей, по низким ценам, по всему миру!

Заграничные паспорта, сроком на 5 и 10 лет ОВИР, МИД.

ТЕЛ: (495)227_04~37
ТЕЛ: (495)227~04+38

Скидки для корпоративных и постоянных клиентов!!!

ЗАГРАНИЦА ЖДЕТ ВАС!

Figure 7 - Typical recent Xarvester email

Xarvester had been responsible for sending a large volume of spam in 2009, but it did not become the giant that everyone expected after it first appeared in January 2009; it had an estimated 500,000-800,000 bots under its control and was responsible for more than 32.1% of all spam at its peak in March 2009.

Continent	Distribution of Bots
Europe	46.2%
Asia	21.4%
South America	17.9%
North America	8.7%
Africa	2.3%

Figure 8 – Geographical distribution of Xarvester botnet

By the end of 2009, Xarvester had an estimated 20,000-36,000 bots under its control, and was responsible for less than 1% percent of all spam. In April 2010, Xarvester was believed to consist of just 10,000 bots, a shadow of its former self. The top five countries where Xarvester bots are located include: Brazil 13.3%, Poland 10.4%, Czech Republic 9.8%, India 9.3% and Russian Federation 5.8%.

The remaining newer botnets, Maazben and Festi, although smaller, may perhaps be considered more successful. Maazben appeared in March 2009, and has maintained a consistent spam output rate per minute ever since. The most dominant it has ever been was during September and October 2009, when it was responsible for about 3% of all spam. The top five countries where Maazben bots are located include: Brazil 32.8%, Vietnam 9.2%, Indonesia 7.0%, India 7.0% and Russian Federation 3.2%.

Continent	Distribution of Bots
South America	35.9%
Asia	33.9%
Europe	18.6%
North America	5.5%
Africa	4.3%
Oceania	0.1%

Figure 9 – Geographical distribution of Maazben botnet

Maazben has been sending mostly French and German casino-related spam, and like Donbot and Xarvester, seems to have faded from approximately 240-340 thousand bots in November 2009, to 40-60 thousand bots in April 2010. Currently, Maazben is actually larger than Donbot and Xarvester combined.

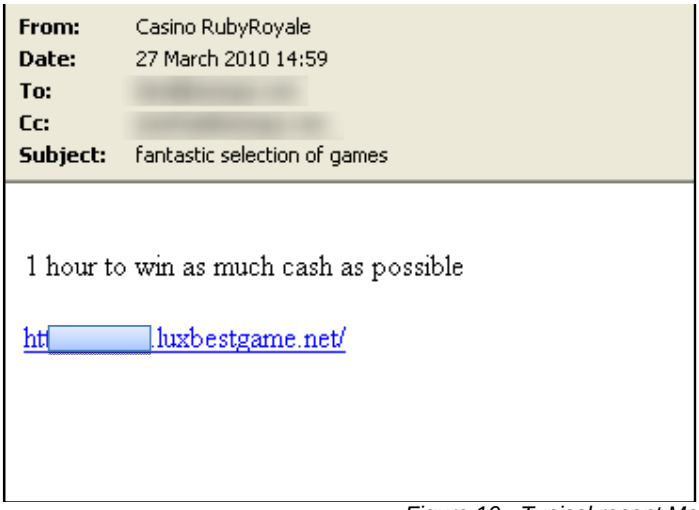


Figure 10 - Typical recent Maazben email

Festi, another of the newer botnets, appeared in August 2009 and has also sustained a steady output, although to date its heyday was in September and October 2009.

In November 2009, Festi was estimated to comprise approximately 140-220 thousand bots, but it has now shrunk to just ten thousand bots.

The only other new botnet of note is Lethic. MessageLabs Intelligence began tracking Lethic at the end of 2009, when it first appeared. Initially, the internet security community became aware of it very quickly and action by Neustar and other ISPs appeared to kill the botnet.

Continent	Distribution of Bots
Europe	45.8%
Asia	27.9%
South America	10.8%
North America	8.1%
Oceania	3.2%
Africa	2.3%

Figure 11 – Geographical distribution of Lethic botnet

However, in March 2010, Lethic returned, when it accounted for 2.1% of all spam on March 14, 2010 and was estimated to comprise 210-310 thousand bots. The top five countries where Lethic bots are located include: The Netherlands 15.1%, UK 7.6%, Israel 6.6%, India 5.8% and Brazil 5.6%.

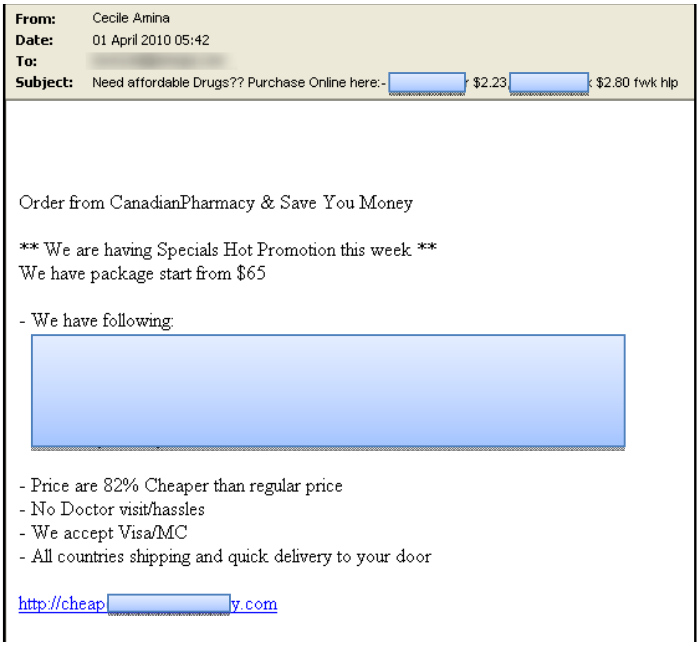


Figure 11 - Typical recent Lethic email

By April 2010, Lethic, Maazben, and Xarvester were the only remaining active botnets that first appeared in 2009. Combined, these three botnets are now responsible for approximately 2% of all spam, with the majority coming from Lethic, with an estimated 210-310 thousand bots at its disposal.

In contrast, Rustock currently sends 32% of all spam, with an estimated 1.6-2.4 million bots under its control, demonstrating that Maazben, Lethic and Xarvester are now really very small.

Infected Operating Systems: Fingerprinting spam-sending botnets – Identifying the operating systems behind the botnets

Passive fingerprinting (PF) of operating systems is unlike active fingerprinting, which sends abnormal packets to a remote host and analyses the responses, going undetected by the remote host. Instead, it analyses the network traffic from the remote host when it attempts to establish a connection and this traffic can be used to identify the operating system in place on the remote machine.

In April, MessageLabs Intelligence analyzed the PF signatures of spam email traffic in order to get an idea of the types of operating systems that were running on the infected spam-sending computers. As expected, most of the PF signatures suggested that many of the infected machines were running Windows, but the levels were not as high as we first imagined. In fact, the percentage of spam with a Windows PF signature was similar to the Windows share of the operating system market.

Botnets generally appeared far more on Windows machines than any other operating system. Once a successful botnet is created, it may spread more rapidly through Windows machines as there are so many of them. It is much more difficult to

spread an infection for any other type of operating system simply because there are far fewer of them.

Figure 12 below, shows the percentage of spam that is from a machine running a Windows operating system, comparing botnet spam, non-botnet spam, and all spam.

	Nov 2009	Dec 2009	Jan 2010	Feb 2010	Mar 2010	Average
All Spam	92.8%	92.7%	92.1%	93.2%	92.6%	92.7%
Non-Botnet	73.4%	86.9%	80.1%	88.0%	72.8%	80.3%
Botnet	96.6%	96.8%	96.5%	96.7%	96.6%	96.6%

Figure 12 – Spam sent from computers running Windows OS

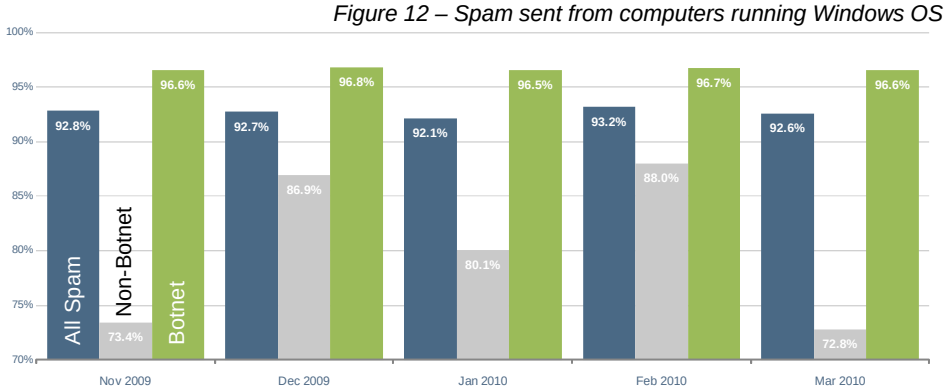


Figure 13 – Spam by source (botnet vs. non-botnet)

As can be seen in figure 13 above, spam is more commonly sent from computers running Windows than from those running other operating systems; however, what may be more interesting is that spam not identified as coming from botnets has a much lower proportion coming from Windows machines than from known botnets.

Figure 14, shows a more detailed chart highlighting the average rates for the top botnets over the previous five months:

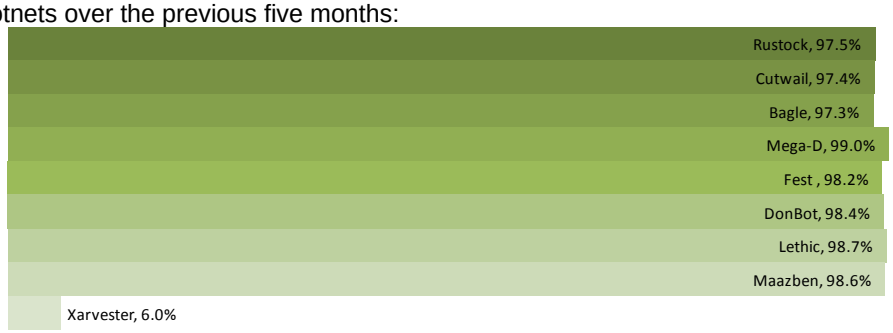


Figure 14 – Average spam rates for top spam-sending botnets

Interestingly, the Xarvester botnet, previously one of the top global spamming botnets, has sent only 6% of its spam from Windows machines since November 2009. The remainder has been sent almost entirely (93.3%) from machines using the Solaris OS.

Currently the Xarvester botnet is far smaller than it used to be. At its height, Xarvester had almost a million bots under its control, but by April 2010, this number dropped to around ten thousand. It is possible that the malware behind the Xarvester botnet has been largely eliminated for Windows, leaving only the non-Windows bots still functional.

	Nov 2009	Dec 2009	Jan 2010	Feb 2010	Mar 2010	Average
Rustock	98.5%	98.3%	98.1%	97.7%	95.2%	97.5%
Cutwail	97.3%	97.3%	97.7%	96.9%	97.6%	97.4%
Bagle	97.7%	98.2%	96.5%	97.5%	96.6%	97.3%
Mega-D	98.5%	100.0%	98.8%	98.7%	98.9%	99.0%
Festi	98.3%	97.9%	98.0%	97.9%	99.0%	98.2%
DonBot	98.9%	98.6%	98.9%	98.7%	96.9%	98.4%
Lethic	96.7%	98.8%	99.1%	100.0%	99.0%	98.7%
Maazben	98.8%	99.2%	98.8%	98.9%	97.2%	98.6%
Xarvester	4.2%	6.3%	5.0%	6.6%	7.7%	6.0%
Overall	92.9%	92.6%	92.1%	92.9%	92.0%	92.5%

Figure 15 – Proportion of spam sent from computers running Windows OS

If we look at all spam from the period November 2009 to March 2010, and break it down by the operating system in place on the sending machine, then we get the following results.

	OS % of Spam
Windows	92.65%
Linux	5.14%
Other	2.22%
MacOS	0.00%

Figure 16 - Proportion of spam sent by OS

The percentage of spam by itself doesn't look very surprising. However, what is particularly interesting is if we compare this information to the operating system market shares. As of April 2010, the following are the market shares[2] for each operating system.

	OS Market Share
Windows	91.58%
MacOS	5.33%
Linux	1.03%
Other	2.06%

Figure 17 - Market share of operating system

Furthermore, by calculating a ratio of spam from a given operating system compared to the market share, we can get a "spam index" which shows relative to its market share, the likelihood that a particular computer is sending spam, based on its operating system. In the current spam climate, this index shows that relative to its market share, any given Linux machine is five times more likely to be sending spam than any given Windows machine.

	SpamIndex (%Spam / MarketShare)
Windows	1.01
Linux	4.99
MacOS	-
Other	1.08

Figure 18 - Likelihood of a computer running an OS sending spam

Whilst this may sound like a surprising statistic, it's worth remembering that Linux machines are only responsible for 5.1% of all spam.

[2] *http://marketshare.hitslink.com/os-market-share.aspx?qprid=9*

Linux is often associated with less risk as an operating system than Windows, and by virtue of its lower market share there are fewer examples of malware in circulation that specifically target the Linux operating system. However, it may be that Linux machines are equally as vulnerable, perhaps through drive-by attacks targeting vulnerabilities in browser plug-ins.

More ISPs are now forcing their clients to route email traffic through the ISPs own "smarthost", a mail server provided for their customers, rather than permit the client to send email directly using TCP port 25. Many such ISPs employ a hosted environment where the operational costs can be lowered through the use of open source technology, such as Linux.

Much of this spam is also likely to include what may be considered more legitimate direct marketing emails that have been blocked as spam, particularly in compliance with legislation such as the CAN-SPAM Act 2003 in the US.

The MacOS is least likely to be sending spam both on its global contribution to spam and on an individual machine basis. These numbers, at this level of precision, suggest that there is almost no spam being sent from MacOS machines. However, this is not quite the case as 0.001% of the spam examined did originate from machines detected as having MacOS.

Also, these numbers do not take into account that many owners of non-Windows machines may be using a virtual machine environment, running with a Windows OS subsystem, perhaps for email purposes. In such cases they may not bother to take proper security precautions for the virtual machine environment. It is equally as important to safeguard a Windows virtual machine connected to the internet as it is for any other environment; the fact that it may be running in a virtual environment is irrelevant.

Ten years on – How the LoveBug virus changed the threat landscape we know today

On May 4, 2000 a virulent worm caught many security experts by surprise and wreaked havoc on an estimated 45 million email users in the course of just one day. With virus levels surging overnight from 1 in every 1,000 emails to 1 in 28, the mass-mailing virus, LoveBug, was on the cusp of causing billions of dollars in damage.

Symantec Hosted Services, then MessageLabs, was the first company to intercept the new virus on 4 May at 12:14 a.m. (British Summer Time). It had been launched from the Philippines and started to wreak global damage as more countries came online to begin their working day. Emails with the subject line 'ILOVEYOU' dropped into inboxes across the world.

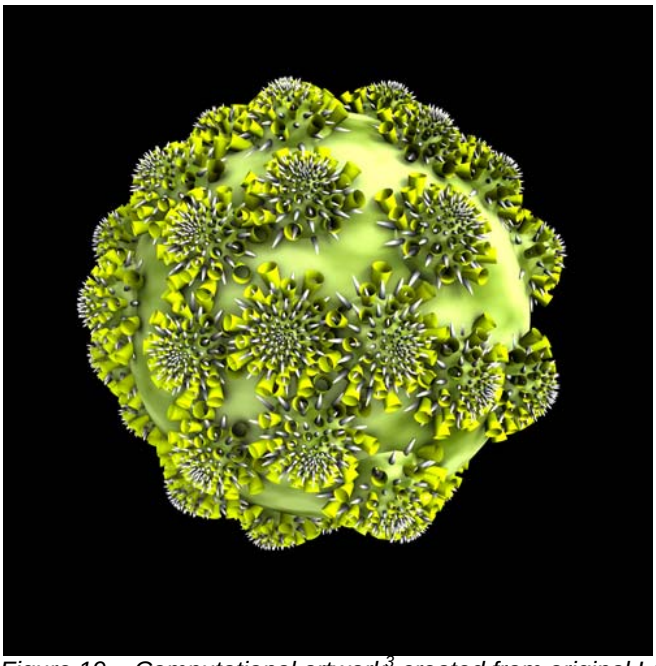


Figure 19 – Computational artwork[3] created from original LoveBug code

Many recipients, who were unable to contain their curiosity over this message from a mystery admirer, opened the attachment which appeared to be a 'safe' text file. For those who were not protected by MessageLabs cloud-based services, once opened, the attachment contained malicious VBScript that sent itself to every email address in the recipient's address book.

```
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObj3ct("WScript.Shell")
rr=wscr.RegR3ad("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWr1te "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFile(WScript.Scr1ptFullName)
c.Copy(dirsystem&"\MSKernel32.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
regruns()
html()
spreadtoemail()
listadriv()
end sub
sub regruns()
```

Figure 20 – Extract of VBScript code from LoveBug

At 7 a.m. BST, eight copies had been caught by Skeptic™, Symantec Hosted Services' heuristic detection engine. Over the following hour that number rose to 462. By 9 a.m., over 3,083 copies of the worm were blocked, more than ten times the number stopped in an average day at that time. By 10 a.m., anti-virus signatures started to become available – close to ten hours after the first copies had been stopped. However, the demand for signatures became so great that nobody could log onto the web servers that were hosting these updates. In many cases it would have been too late anyway; the damage had already been done.

[3] *For more information about the artwork and the process used to create it, see http://www.messagelabs.com/threats*

In the days that followed, copycat viruses and toolkits were used to generate similar scripted malware, but these were also blocked by Skeptic™, because it was able to learn from what had gone before.

By midnight, more than 13,000 copies had been blocked. At the time, Skeptic was processing over 2 million emails each day, compared with over 570 million processed per day on average in April 2010. Skeptic now routinely blocks more than 1.5 million emails each day as malicious.

In 2000, cyber criminals were only just learning to harness the powers of the early internet, disrupting services and causing damage to businesses and email systems. LoveBug followed in the wake of the Melissa virus in 1999, a similarly destructive worm which spread rapidly through users' email accounts. Ten years ago, users did not have the same understanding of internet threats as we do today; few perceived the dangers posed by suspicious email attachments or emails from unknown senders.

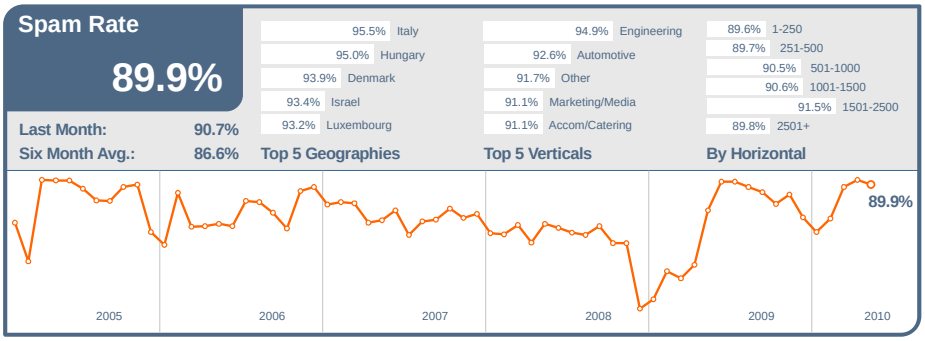
As the internet has evolved, so have the criminals' techniques. Today, we typically focus on more malicious, highly targeted attacks. Cyber criminals have turned their attention from developing and spreading malicious code for increasing kudos and credibility amongst their peers, to financial gain and stealing users' online identities for profit. Social media is also in the criminals' gaze today, as these sites continue to attract growing numbers of users. Attacks designed to exploit a certain operating system or platforms are often related to that platform's market share.

As a result of the LoveBug virus, legislation in the Philippines was changed and today some highly effective legislature exists to combat online crime. Precisely what threats will be contemporary in the next ten years is unclear, but we do know that criminals are likely to continue to find new ways to exploit the internet and the technology that has grown up around it.

GLOBAL TRENDS & CONTENT ANALYSIS

MessageLabs Hosted Email AntiSpam and Hosted Email AntiVirus 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 2010, the global ratio of spam in email traffic decreased by 0.8 percentage points since March to 89.9% (1 in 1.11 emails).



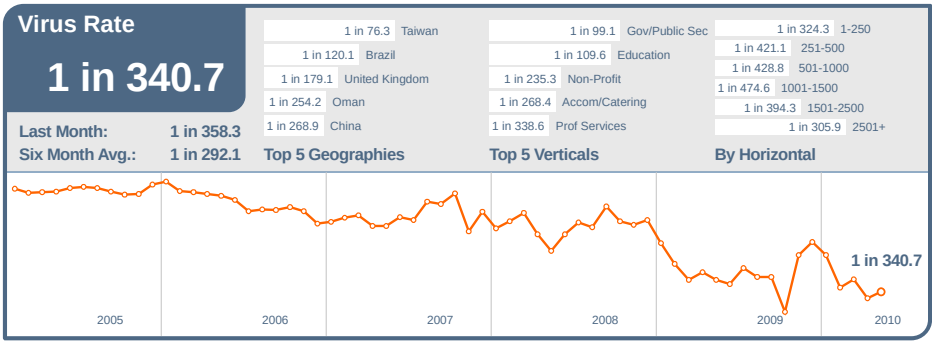
April 2010

The spam level in Italy rose to 95.5% of email traffic during April, making it the most spammed country. In the US, 90.2% of email was spam and 88.9% in Canada. The spam level in the UK was 89.4%. In The Netherlands, spam accounted for 91.5% of email traffic, 92.3% in Germany and 89.4% in Australia. In Hong Kong, 91.0% of email was blocked as spam and 87.6% in Singapore, compared with 86.9% in Japan and 91.6% in China.

In April, the most spammed industry sector with a spam rate of 94.9% was the Engineering sector. Spam levels for the Education sector reached 91.1% and 90.2% for the Chemical & Pharmaceutical sector; 90.7% for IT Services, 90.9% for Retail, 88.4% for Public Sector and 88.4% for Finance.

Skeptic™ Anti-Virus and Trojan Protection: The global ratio of email-borne viruses in email traffic was 1 in 340.7 emails (0.294%) in April, an increase of 0.01 percentage points since March.

In April, 28.9% of email-borne malware contained links to malicious websites, an increase of 12.1 percentage points since March.



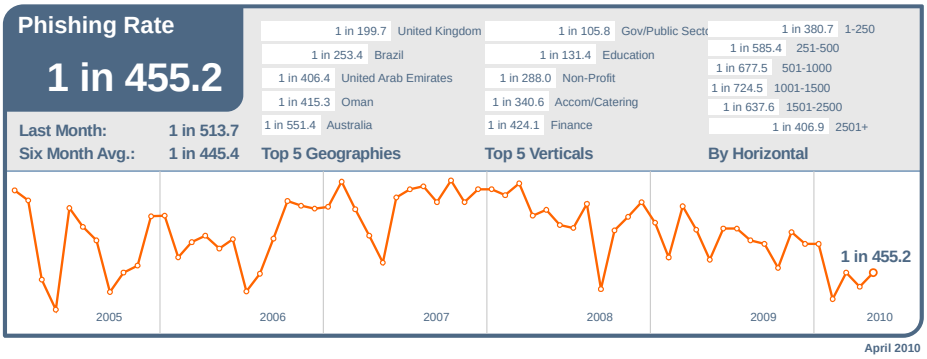
April 2010

In April, 1 in 76.3 emails destined for Taiwan was blocked as malicious, ensuring the country remains the most targeted for email-borne malware. The virus levels for malware in email traffic in the US was 1 in 646.3 and 1 in 416.2 for Canada. In Germany virus activity reached 1 in 471.0 and in The Netherlands was 1 in 1,120. In Australia, 1 in 416.5 emails were malicious and 1 in 501.0 in Hong Kong; for Japan it was 1 in 1,161.0, compared with 1 in 613.0 in Singapore.

The Public Sector remained the most targeted industry in April, with 1 in 99.1 emails being blocked as malicious. Virus levels for the Chemical & Pharmaceutical sector were 1 in 438.2 and 1 in 487.5 for the IT Services sector; 1 in 600.2 for Retail, 1 in 109.6 for Education and 1 in 365.9 for Finance.

Email virus	%
Exploit/MimeBoundary003	11.4%
Trojan.Bredolab	11.0%
Link-W32/NewMalware-bc37	5.1%
Exploit/Fraud-AccUpdate	4.9%
W32/Prolaco-gen-4b33	3.6%
Exploit/LinkAliasPostcard-fd78	3.5%
Trojan.Sasf s.dam	2.1%
Exploit/LinkAliasPostcard-74a5	2.0%
Trojan.Bredolab!eml	1.6%
Link-Suspicious.DLoader-3631	1.3%

Phishing: In April, phishing activity rose by 0.03 percentage points since March; 1 in 455.2 emails (0.219%) comprised some form of phishing attack. When judged as a proportion of all email-borne threats intercepted in April, including viruses and Trojans, the proportion of phishing emails rose by 5.7 percentage points to 70.3% of all email-borne malware and phishing threats combined.



The UK continued to receive the most phishing emails in April, with 1 in 199.7 emails comprising a phishing attack. Phishing levels for the US were 1 in 1,216 and 1 in 813.5 for Canada. In Germany phishing levels were 1 in 1,607 and 1 in 2,626 in The Netherlands. In Australia, phishing activity accounted for 1 in 551.4 emails and 1 in 1,640 in Hong Kong; for Japan it was 1 in 5,165 and 1 in 3,300 for Singapore.

The Public Sector remained at the top of the table with 1 in 105.8 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were 1 in 750.0 and 1 in 888.4 for the IT Services sector; 1 in 853.0 for Retail, 1 in 131.4 for Education and 1 in 424.1 for Finance.

Skeptic™ Web Security Version 2.0: The most common trigger for policy-based filtering applied by the MessageLabs Hosted Web Security Service for its business clients was the "Advertisements & Popups" category, down by 1.6 percentage points since March, to 51.2% in April.

The largest increase in policy blocks, of 0.81 percentage points, was for the Personals & Dating category, which includes many social networking websites. The blocking of Unclassified websites decreased by 0.78 percentage points. The Unclassified category identifies new and previously uncategorized websites. While these websites can be used for disreputable purposes, such as hosting phishing and spam sites, they may also be new sites and domains set up by legitimate organizations in the process of being categorized. Customers are able to adopt a more flexible approach to how these websites are treated, since all content downloaded is scanned for malware by a unique combination of commercial anti-virus engines and Skeptic technology. This ensures that customers do not need to have a default block on these sites to maintain security, as may otherwise be the case.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	51.2%	Trojan.Zbot!gen2	9.4%	PUP:Win32.Zwangi.qm	28.9%
Streaming Media	9.8%	New Unclassified Worm	3.8%	PUP:Lop	21.8%
Downloads	4.2%	Trojan-Downloader.JS.Gumblar.a	3.6%	PUP:ZangoSearch	17.1%
Games	3.9%	New Unclassified Trojan	3.3%	PUP:WebToolbar.Win32.MyWeb...	5.3%
Personals & Dating	3.8%	Trojan-Downloader.JS.Gumblar.x	3.3%	PUP:Win32.FunWeb.di	3.4%
Unclassified	3.6%	Backdoor.Trojan	3.2%	PUP:Win32.BHO.lku	3.0%
Blogs & Forums	2.9%	Trojan.Malscript!html	2.8%	PUP:Win32.FunWeb.ar	2.7%
Search Engines	2.8%	Exploit/Phishing-hmrc-ee11	2.6%	PUP:Adhelper	1.5%
Computing & Internet	2.8%	Bloodhound.PDF!gen	2.5%	PUP:PUP:Win32.BHO.lkh	1.0%
Chat	2.7%	Trojan.JS.Redirector.l	2.3%	PUP:RiskTool.Win32.MBRFix.a	1.0%

April 2010

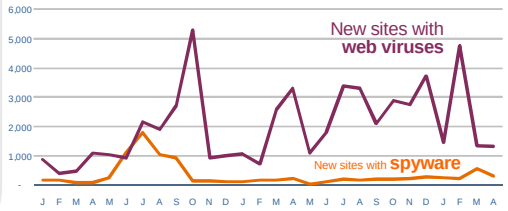
MessageLabs Intelligence identified an average of 1,675 websites each day harboring malware and other potentially unwanted programs including spyware and adware; a decrease of 12.7% since March.

Further analysis also reveals that 33.6% of all malicious domains blocked were new in April; a decrease of 6.3 percentage points compared with March. Additionally, 10.9% of all web-based malware blocked was new in April; a decrease of 4.0 percentage points since the previous month.

The chart below shows the increase in the number of new spyware and adware websites blocked each day on average during April compared with the equivalent number of web-based malware websites blocked each day.

Web Security Services (Version 2.0) Activity:

New Malware Sites per Day	
New sites with **spyware**	334/day
New sites with **web viruses**	1,341/day
Total	**1,675/day**

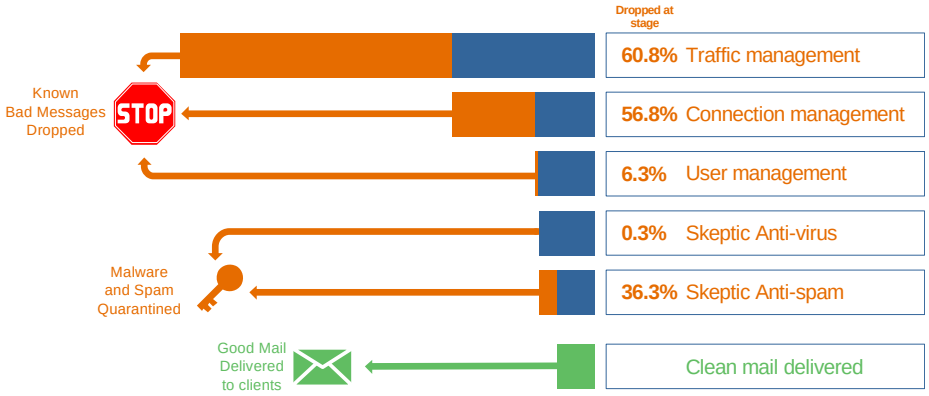


April 2010

TRAFFIC MANAGEMENT

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 April, MessageLabs services processed an average of 12.3 billion SMTP connections per day, of which 60.8% were throttled back as a result of traffic management controls for traffic that was unequivocally malicious or unwanted. The remainder of these connections was subsequently processed by MessageLabs Connection Management controls and Skeptic™.



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, using SMTP Validation techniques. It is able to identify 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, an average of 56.8% of inbound messages was intercepted from botnets and other known malicious sources and rejected as a consequence.

User Management

User Management uses Registered User Address Validation techniques to reduce the overall volume of emails for registered domains, by discarding connections for which the recipient addresses are identified as invalid or non-existent. In April, an average of 6.3% of inbound messages was identified as invalid; these were attempted directory attacks upon domains that were therefore prevented.

About MessageLabs Intelligence
MessageLabs Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. MessageLabs Intelligence publishes a range of information on global security threats based on live data feeds from more than 14 data centers around the world scanning billions of messages and web pages each week. MessageLabs Team Skeptic™ comprises many world-renowned malware and spam experts, who have a global view of threats across multiple communication protocols drawn from the billions of web pages, email and IM messages they monitor each day on behalf of 30,000 clients in more than 100 countries. More information is available at www.messagelabs.com/intelligence.

About Symantec
Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. More information is available at www.symantec.com.