MessageLabs Intelligence:
2010 Annual Security Report

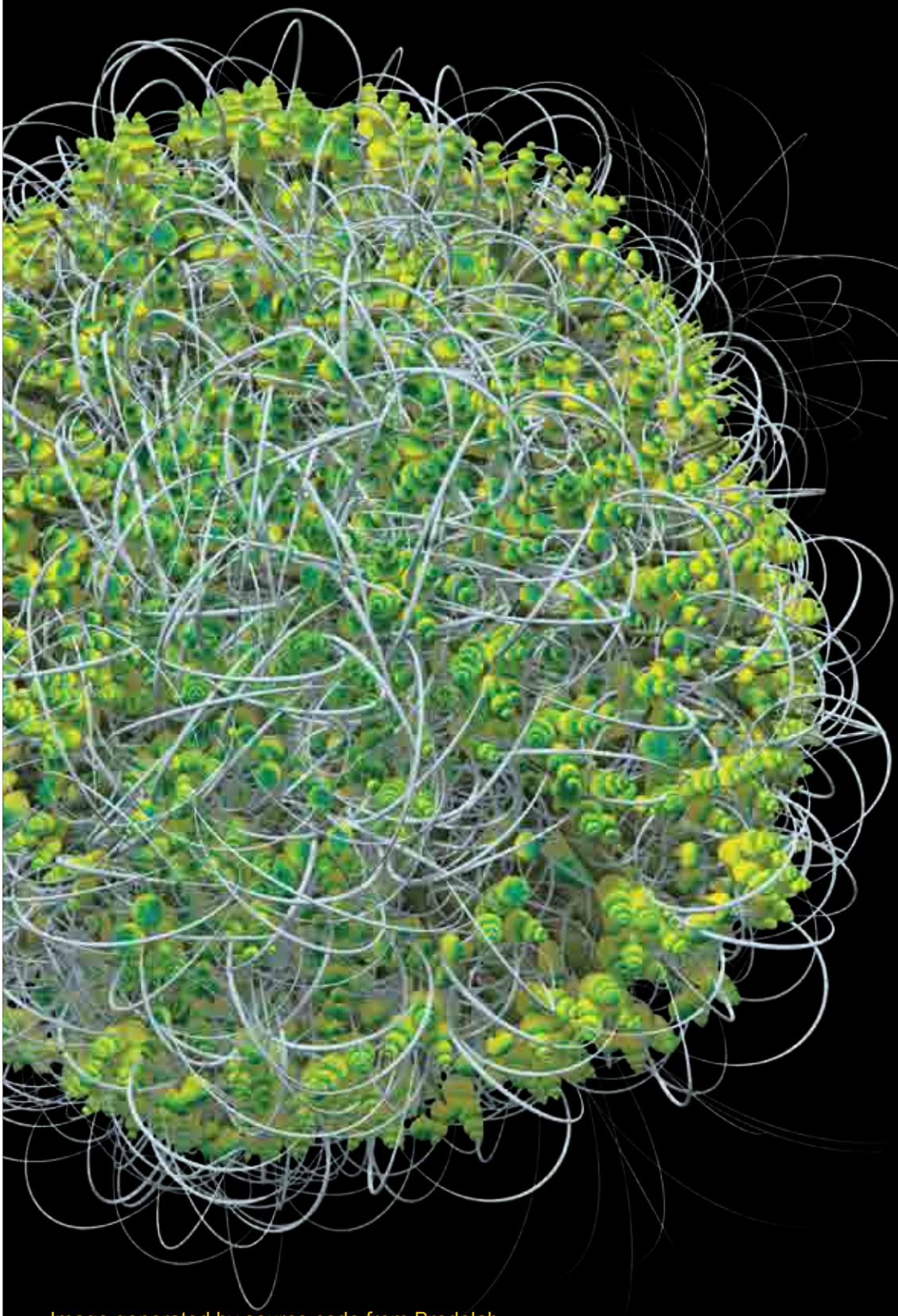


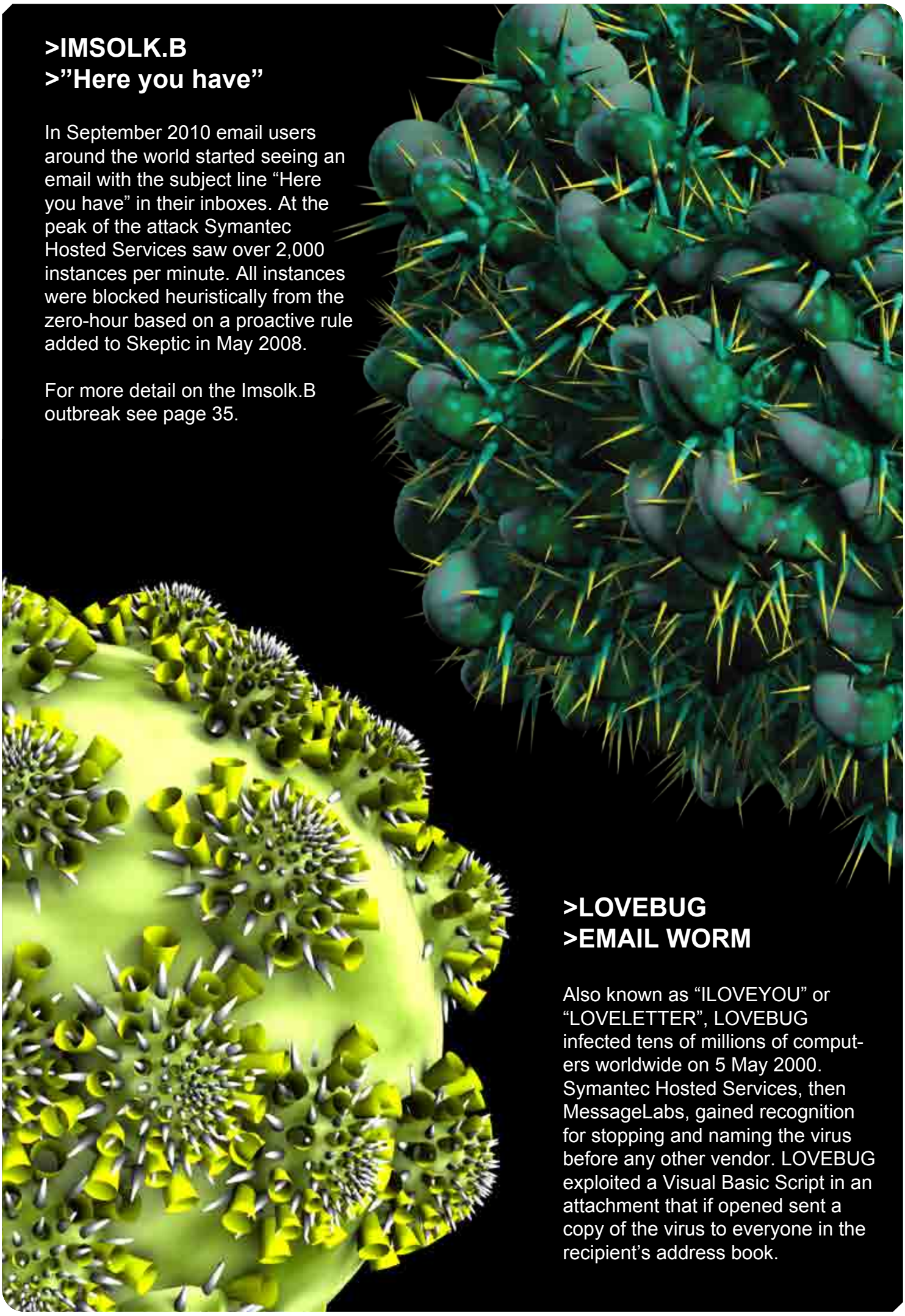
Image generated by source code from Bredolab

Hosted Services
by Symantec™

>IMSOLK.B
>”Here you have”

In September 2010 email users around the world started seeing an email with the subject line “Here you have” in their inboxes. At the peak of the attack Symantec Hosted Services saw over 2,000 instances per minute. All instances were blocked heuristically from the zero-hour based on a proactive rule added to Skeptic in May 2008.

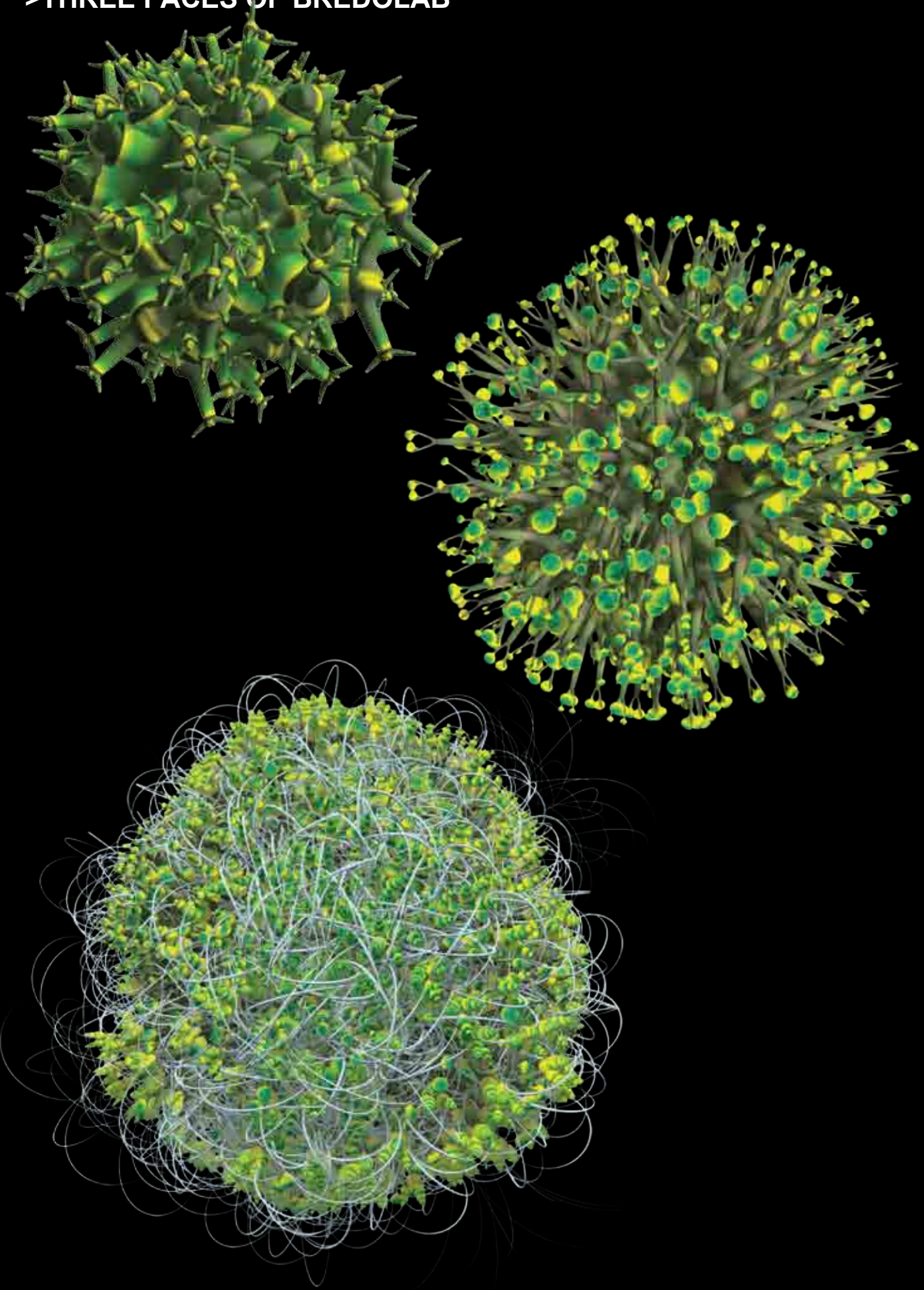
For more detail on the Imsolk.B outbreak see page 35.



>LOVEBUG
>EMAIL WORM

Also known as “ILOVEYOU” or “LOVELETTER”, LOVEBUG infected tens of millions of computers worldwide on 5 May 2000. Symantec Hosted Services, then MessageLabs, gained recognition for stopping and naming the virus before any other vendor. LOVEBUG exploited a Visual Basic Script in an attachment that if opened sent a copy of the virus to everyone in the recipient’s address book.

>THREE FACES OF BREDOLAB



For more detail on the development of Bredolab see page 42.

Table of Contents

1 EXECUTIVE SUMMARY

Welcome to the MessageLabs Intelligence 2010 Annual Security Report. In this report we explore the significant developments over the course of the year and their impact on the security landscape; looking ahead into 2011 we provide our insight and analysis of the most important threats and areas to watch in the coming months. In 2010, much of the security landscape was shaped by the technological advances made in more sophisticated forms of malware as the cyber criminals continued to find new and innovative ways to attack computers and businesses. The key points of note from this report include the following:

- In 2010, the average global spam rate for the year was 89.1%, an increase of 1.4% compared with 2009. The proportion of spam sent from botnets was much higher for 2010, accounting for approximately 88.2% of all spam. The largest change in 2010 was a significant shift in spam-sending locations as more spam was sent from Asia and South America at the start of the year, but by the end of the year the majority was sent from Europe, accounting for approximately 30% of global spam. At the end of 2009, 96% of spam sent was in English, but this number has slowly declined during 2010, falling to an all-time low of 90% in August, where it has remained since. Ten percent of spam sent is now in local languages.
- Despite many attempts to disrupt botnet activities throughout 2010, by the end of the year the total number of active bots returned to roughly the same number as at the end of 2009, with approximately five million spam-sending botnets in use worldwide. However, the average number of spam emails sent from each bot fell from approximately 85 emails per bot per minute in 2009 to approximately 77 spam emails per bot per minute at the end of 2010. This led to a decrease in the total amount of global spam in circulation toward the end of 2010. There were some exceptions however, particularly with Rustock, which continued to dominate and was responsible for 47.5% of all spam at the end of the year.
- In 2010, spammers and scammers produced many spam campaigns relating to major newsworthy events. While the particular events may only have national or regional appeal, the approaches that spammers and scammers use were often similar. Major sporting events like the FIFA World Cup, which took place in South Africa in June 2010, were exploited by spammers. Before, during and after the event, MessageLabs Intelligence identified a wide variety of different threats relating to the FIFA World Cup, including spam, scams and advance-fee “419” fraud, and malware attacks. The spammers’ use of URLs from link-shortening services became increasingly popular during 2010, most notably on April 30 when approximately 18.0% of spam that day contained a shortened URL. An average of 91% of all spam contained some kind of URL in 2009 and in 2010 this figure was almost unchanged at 91.1%. Approximately 0.33% of all spam contained a short URL in 2009, compared with 1.38% (1 in 72.5) in 2010.
- In 2010, the average rate for malware in email traffic was 1 in 284.2 emails (0.352%), almost unchanged when compared with 1 in 286.4 (%) for 2009. Approximately 23.7% of malware blocked in 2010 contained a malicious link within the body of the message, compared with 15.1% in 2009. In 2010, there were over 339,600 different malware strains identified in emails blocked, representing over a hundredfold increase compared with 2009. This is largely due to the growth in polymorphic malware variants, typically generated from toolkits that allow a new version of the code to be generated quickly and easily.

An example of this is the Bredolab family of general-purpose Trojans, linked with the Pandex and Cutwail botnets, which accounted for approximately 7.4% of all email-borne malware in 2010.

- In 2010, the Stuxnet Trojan made tangible the potential for malware to materially impact industrial control system hardware and cause significant disruption beyond cyberspace. The "Here You Have" virus (a.k.a. W32.IMSOLK.B@mm) in September also showed that old-style mass mailer viruses can still prove effective and demonstrated that even after 25 years, the signature-based approach of anti-virus countermeasures is still inadequate. With Skeptic™ and its 10 year pedigree of proactive security in the cloud, Symantec was able to protect its MessageLabs clients against this attack. The outbreak was over by the time many other security vendors issued protection.
- The threat from targeted email attacks - which have the ultimate aim of gaining access to specific sensitive data, corporate intellectual property or access to confidential internal systems – has not diminished in 2010. These are sent in low volumes, targeting specific individuals within organizations, but are potentially one of the most damaging threats any organization can face. By the end of 2010, MessageLabs Intelligence identified approximately 77 targeted attacks blocked each day, compared with 48 per day for 2009.
- In 2010, the average ratio of email traffic blocked as phishing attacks was 1 in 444.5 (0.23%), compared with 1 in 325.2 (0.31%) in 2009. More than 188.6 million phishing emails were blocked by Skeptic™ in 2010. Approximately 95.1 billion phishing emails were estimated to be in circulation during 2010. In 2010, MessageLabs Intelligence tracked phishing attacks impersonating or relating to 1,530 different organizations, compared with 1,079 in 2009. In 2010, impersonations of five organizations made up 50% of all phishing attacks, as compared with eight in 2009. The most frequently spoofed phishing organization was a well-known international bank, accounting for 14.9% of phishing attacks blocked in 2010. The second most frequently blocked phishing attacks impersonated a large online retailer. Spear phishing against businesses, where the sender's address was forged to appear as though it were sent from an internal employee, accounted for 6.3% of all phishing emails blocked in 2010.
- In 2010, the average number of web sites blocked as malicious each day rose to 3,188 compared with 2,465 in 2009; an increase of 29.3%. In 2010, MessageLabs Intelligence identified malicious web threats on 42,926 distinct domains, the majority of which were compromised legitimate domains. In 2010, the threat posed by the web is more acute and extensive than before. Almost any web site can now be used to host malware or redirect visitors to one that does. Indeed, an infection is much more likely to result from a visit to a perfectly legitimate web site that has been compromised with a virus or spyware than from one set up specifically to spread malware. In addition, techniques such as drive-by downloads have become commonplace, where simply visiting an infected site is enough to infect a computer. In 2010, almost 90% of malicious web sites blocked are legitimate, compromised web sites.
- One of the greatest challenges for IT managers in recent years has been how to secure an increasingly mobile workforce. In 2010, MessageLabs Intelligence analysis identified high-risk behavior profiles when staff are roaming versus in the office; 35% of users that were both office-based and mobile had a higher proportion of web requests blocked by the MessageLabs Web Security service when roaming, compared to when in the office. For all employees browsing the web, approximately one in five requests were blocked, but behavior differs

widely from employee to employee. It is therefore important to understand which employees present the greatest level of risk to an organization. For example, 20% of users had more web page requests blocked than allowed, and the highest risk, 14% of users, had between 90-100% of all requests blocked.

- As social media and Web 2.0 applications have grown in participant numbers and capability over the last few years, public and private social media tools have become increasingly relevant to businesses. Likewise, cyber criminals have recognized opportunities to conduct their criminal activity in new and interesting ways. In 2010, many social networking platforms and social media web sites were being routinely abused and exploited; for example, by providing a rich seam from which personal information can be tapped about an individual in reconnaissance as a prelude to a more targeted attack. Social networking web sites are being phished to gain access to real accounts and there have been instances reported where rogue third-party “apps” have been created that may subsequently be added to users’ profile pages. Even legitimate apps may be vulnerable to being exploited where vulnerabilities may exist in the web site in just the same way as many other legitimate web sites have also been compromised and used to host malware

We hope you enjoy reading this year’s report!

2 AT A GLANCE: 2010 IN REVIEW

Threat Landscape: Detected by MessageLabs Services

Email spam intercepted

2010
Global spam rate
89.1%

Top 5 Geographies

93.5%	Italy
93.2%	Denmark
92.0%	Austria
92.0%	France
91.5%	Switzerland

Top 5 Verticals

93.5%	Engineering
93.0%	Automotive
91.3%	Accom/Catering
91.2%	Marketing/Media
91.0%	Education

By Horizontal

89.7%	1-250
90.1%	251-500
90.4%	501-1000
90.2%	1001-1500
91.3%	1501-2500
90.1%	2501+

Email virus intercepted

2010
Global virus rate
1 in 284.2

Top 5 Geographies

1 in 147.2	South Africa
1 in 164.6	United Kingdom
1 in 174.1	Spain
1 in 229.0	Oman
1 in 237.8	Switzerland

Top 5 Verticals

1 in 70.5	Gov/Public Sector
1 in 158.6	Education
1 in 185.3	Engineering
1 in 238.9	Marketing/Media
1 in 276.6	Prof Services

By Horizontal

1 in 290.2	1-250
1 in 336.9	251-500
1 in 329.6	501-1000
1 in 379.0	1001-1500
1 in 302.5	1501-2500
1 in 261.3	2501+

Email phish intercepted

2010
Global phish rate
1 in 444.5

Top 5 Geographies

1 in 99.0	South Africa
1 in 214.8	United Kingdom
1 in 341.9	Oman
1 in 424.0	United Arab Emirates
1 in 568.1	New Zealand

Top 5 Verticals

1 in 104.3	Gov/Public Sector
1 in 207.8	Education
1 in 367.4	Marketing/Media
1 in 379.7	Non-Profit
1 in 381.4	General Services

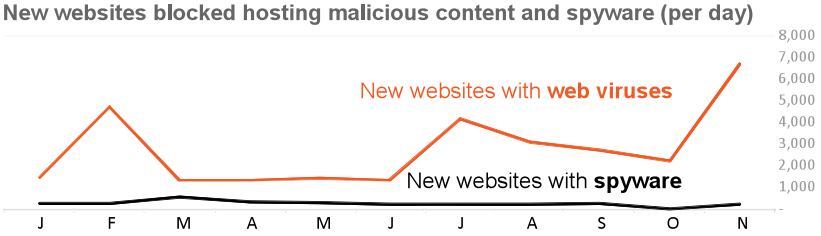
By Horizontal

1 in 375.3	1-250
1 in 575.8	251-500
1 in 575.8	501-1000
1 in 685.4	1001-1500
1 in 599.9	1501-2500
1 in 407.9	2501+

Web malware and spyware

2010
New sites with malware
3,066
/day

New websites blocked hosting malicious content and spyware (per day)



3 SPAM: TOP THREATS OF 2010

3.1 Spam Summary

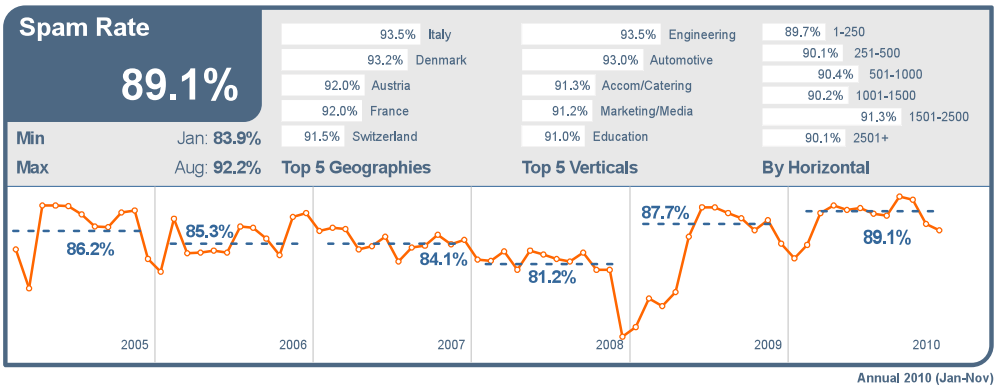


Figure 1 Spam rate

In 2010, the average global spam rate for the year was 89.1%, an increase of 1.4% compared with 2009. In August 2010, the global spam rate peaked at 92.2% when the proportion of spam sent from botnets rose to 95%, as the Rustock botnet was being aggressively seeded by new malware variants and quickly put to use.

Towards the latter part of 2010, overall spam volumes began to decline. A number of botnets were targeted for takedowns during the year, but none of these efforts resulted in as dramatic a reduction in spam that followed the disconnection of the rogue ISP McColo from the Internet in 2008.

3.2 Botnets Role in Spam

By the end of 2010, spam sent from botnets accounted for approximately 77% of all spam. Output from some botnets including Grum and Mega-D declined and spam from Storm, Lethic and Asprox vanished almost entirely. There was a resurgence in spam from smaller botnets such as Maazben and a lesser-known botnet called Cimbot. The proportion of spam sent from botnets was much higher for much of 2010, accounting for 88.2% of all spam, before trailing off in the last three months of the year.

A botnet, or robot network, is a collection of zombie machines controlled by cyber criminals using a particular strain of malware for each botnet. A botnet Trojan refers to the malware used to create new botnets. Many, but not all botnets are used to send spam. Some, like Zeus, are crafted to conduct financial fraud. The Zeus botnet is never used to send spam but the Zeus Trojan may be downloaded onto a computer already infected with another Trojan, such as Bredolab. For example, the Zeus Trojan is sometimes downloaded alongside the Pandex Trojan, which in turn downloads the Cutwail spam engine used to send spam from the Cutwail botnet.

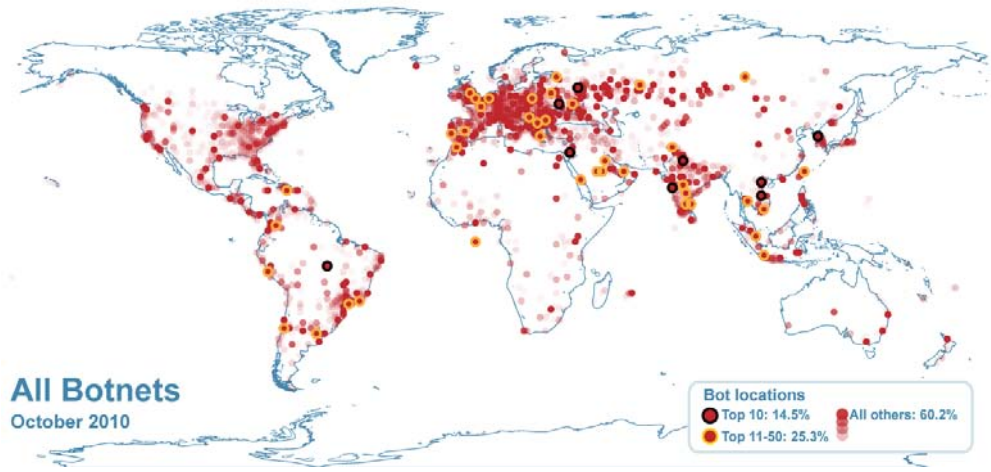


Figure 2 Global bot locations

Botnets generally account for between 80-90% of all spam sent globally. The number of computers recruited to botnets during a particular period has enabled the spam output of almost every country with botnet infected computers to increase its output.

Another significant change in the spam landscape in 2010 is a sizable shift in spam-sending locations, from Asia and South America at the start of the year, to Europe by the end of the year.

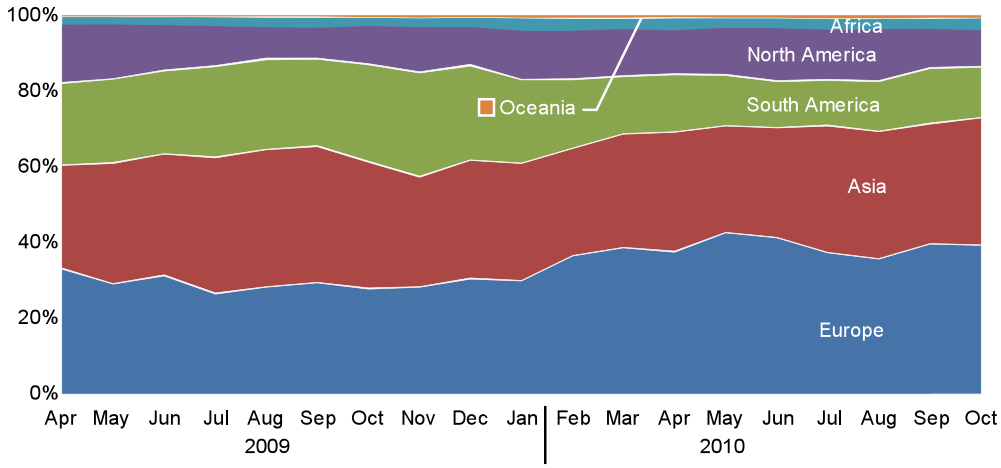


Figure 3 Source of spam sent by continent

3.2.1.1 Europe Extends Lead in Spam Led by Eastern Europe

Europe has always been a significant source of spam and in 2009 it sent similar volumes of spam as Asia and South America did, accounting for approximately 30% of global spam.

However, in 2010, MessageLabs Intelligence has seen Europe increase the amount of spam sent, while spam from South America has decreased and Asia has continued much as before.

Continent	% of global spam
Europe	39.3%
Asia	33.9%
South America	13.4%
North America	9.5%
Africa	3.2%
Oceania	0.7%

Table 1 2010 spam sources

Europe now leads in spam sent (Table 1).

MessageLabs Intelligence performed further analysis to reveal which parts of Europe were mainly responsible for this increase.

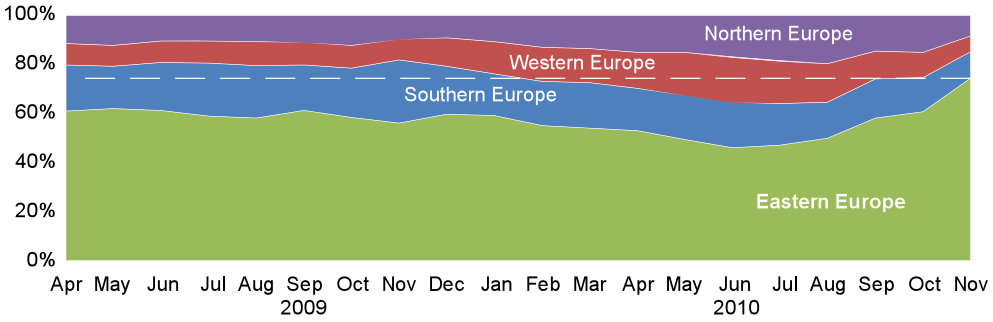


Figure 4 Source of spam within Europe by region

Figure 4 illustrates that the percentage of spam from Europe that comes from Eastern Europe has increased fairly dramatically. It appears the overall increase in global spam originating from Europe is a result of increased spam from Eastern Europe, including Belarus, Bulgaria, Czech Republic, France, Hungary, Republic of Moldova, Poland, Romania, Russian Federation, Slovakia and Ukraine. This is likely due to increased numbers of computers, access to bandwidth, and tactical decisions on the part of cyber criminals.

3.2.1.2 Impact of Getting Connected: Spam from Africa

With increasing broadband availability, and large volumes of users gaining internet access, with little or no protection from malicious threats and little awareness about computer security, new users are quickly becoming infected with malware as their computers are recruited to botnets. Since the rollout of high-speed broadband Internet connections along the Eastern seaboard over the last year or so, botnets have also been successful in Africa recruiting new bots to their operation.

In May 2010, MessageLabs Intelligence published its analysis on the changes in spam from East Africa. The report included some useful links to information about the new broadband connectivity that went live in July 2009 with the deployment of a new fiber optic cable which is still being rolled out in East Africa.[1]

MessageLabs Intelligence revisited the same analysis to investigate the extent to which rates have changed since May. We have used the same definitions for East and West as before, for Group A and Group B respectively as seen in Figure 5.[2]

---

[1] May 2010 MessageLabs Intelligence Report: http://www.messagelabs.com/mlireport/MLI_2010_05_May_FINAL_EN.pdf

2 Group A:African countries served by the cable: Botswana, Burundi, Djibouti, Eritrea, Ethiopia, Kenya, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Rwanda, Seychelles, Somalia, South Africa, Sudan, Swaziland, United Republic of Tanzania, Uganda, Zambia and Zimbabwe.

The proportion of global spam sent from Africa has been steadily increasing, but has not increased dramatically since May. Over the longer term, however, the volume has clearly amplified.

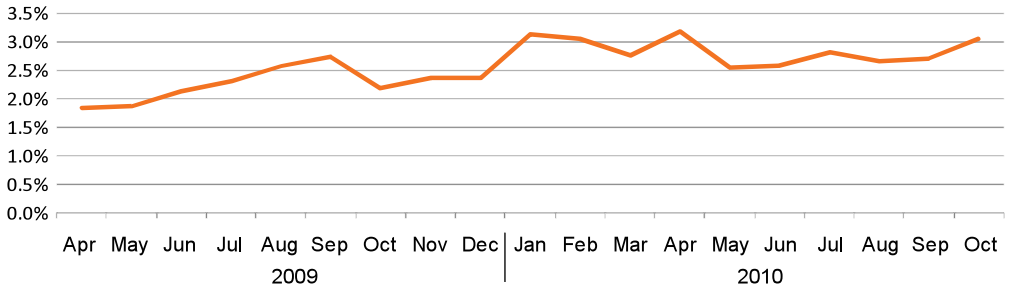


Figure 6 Percentage of global spam originating in Africa

In almost every country from Group A, an increase was noted in the number of distinct botnets sending spam from each country. In April 2009, MessageLabs Intelligence tracked spam from South Africa emanating from seven botnets, today we see spam from 16 different botnets. In Kenya we saw six in April 2009, today we see 14.

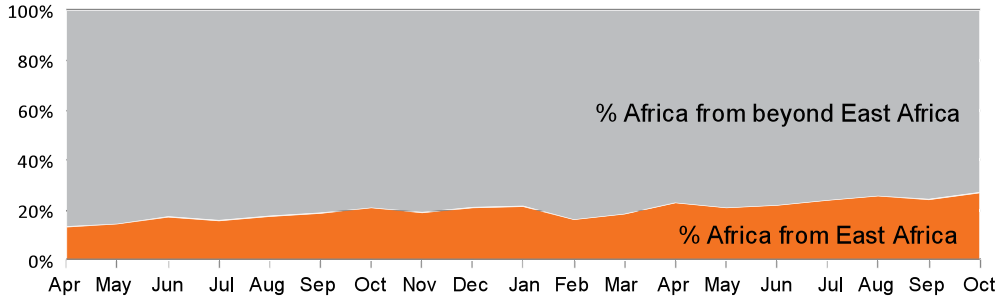


Figure 7 Percentage of spam originating from Group A versus other African countries

As botnets become more powerful globally they are leveraging the opportunity to infect unsuspecting users in Group A countries as they start to use their new broadband connections. Botnets that already had a presence in Group A countries have simply infected more users and grown the number of bots in the region.

The same effect is likely to occur in any region where new users are gaining access to the internet at faster speeds. This presents the cyber criminals behind these botnets with new opportunities to infect new machines and subsequently the region will send increasing volumes of spam.

Group B: Algeria, Angola, Benin, Burkina Faso, Cameroon, Cape Verde, Central African Republic, Chad, Congo, Cote d'Ivoire, Egypt, Equatorial Guinea, Gabon, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Libyan Arab Jamahiriya, Mali, Mauritania, Morocco, Namibia, Niger, Nigeria, Sao Tome and Principe, Senegal, Sierra Leone, Togo and Tunisia.

Country: (in order of biggest increase in spam volume)	% of East Africa spam: April 2009	October 2010	Spam volume sent: Oct2010 / Apr2009
Madagascar	0.9%	2.3%	4.33
Kenya	12.9%	21.0%	4.07
Zambia	1.4%	2.1%	4.03
Rwanda	1.9%	2.7%	2.88
Tanzania	3.8%	5.9%	2.61
Malawi	0.5%	0.7%	1.88
Uganda	2.8%	2.2%	1.83
Mauritius	7.3%	11.8%	1.65
Djibouti	0.7%	1.4%	1.36
Burundi	0.1%	0.3%	1.21
South Africa	47.5%	34.5%	1.02

Country: (in order of biggest increase in spam volume)	% of East Africa spam: April 2009	October 2010	Spam volume sent: Oct2010 / Apr2009
Sudan	10.2%	8.7%	0.88
Zimbabwe	0.8%	0.7%	0.70
Ethiopia	3.0%	1.8%	0.58
Mozambique	3.2%	2.5%	0.54
Botswana	1.9%	0.3%	0.50
Lesotho	0.0%	0.4%	new sender
Seychelles	0.0%	0.4%	new sender
Swaziland	0.0%	0.3%	new sender
Somalia	0.0%	0.1%	new sender
Eritrea	0.0%	0.0%	

Table 2 Spam from select countries in Africa

3.2.2 State of Botnets at the End of 2010

botnet	% of spam	spam/day	spam/ bot/ min	Est. botnet size	Country of Infection
Rustock	47.5%	44.1 billion	145	1100k to 1700k	USA (17%), Brazil (7%), India (7%)
Grum	8.5%	7.9 billion	91	310k to 470k	Russia (12%), India (8%), Vietnam (8%)
Cutwail	6.3%	5.9 billion	40	560k to 840k	India (17%), Russia (16%), Ukraine (8%)
Maazben	5.2%	4.8 billion	37	510k to 770k	Russia (11%), India (10%), Brazil (7%)
Mega-D	2.3%	2.1 billion	105	80k to 120k	Russia (15%), Ukraine (14%), Brazil (7%)
Cimbot	2.1%	1.9 billion	185	32k to 48k	Italy (27%), Spain (25%), France (14%)
Bobax	1.2%	1.1 billion	18	250k to 370k	India (32%), Russia (25%), Ukraine (9%)
Xarvester	0.5%	501 million	109	17k to 25k	Italy (15%), UK (10%), Poland (8%)
Festi	0.1%	96 million	127	8k to 12k	Vietnam (24%), Indonesia (21%), India
Gheg	0.1%	49.8 million	20	8k to 12k	Spain (12%), Indonesia (10%), India (10%)
Other, smaller Botnets	0.5%	26.8 million	22	220k to 340k	
UnNamed Botnets	2.9%	2.6 billion	21	490k to 740k	
Total BotnetSpam	**77.0%**	**71.1 billion**	**77**	**3500k to 5400k**	**India (9%), Rusia (9%), USA (7%)**
Non-botnet spam	**23.0%**	**21.8 billion**			
Grand Total		**92.9 billion**			

Table 3 Botnets October 2010

General

- By the end of 2010, the total number of active bots returned to roughly the same number as at the end of 2009, increasing by approximately 6% in the latter half

of 2010. However, the average number of spam emails sent from each bot fell from approximately 85 emails per bot per minute in 2009 to approximately 77 spam emails per bot per minute at the end of 2009.

- The overall average for 2010 revealed 88.2% of spam was sent from botnets, falling to 77% at the end of 2010, compared with 83.4% of all spam at the end of 2009.

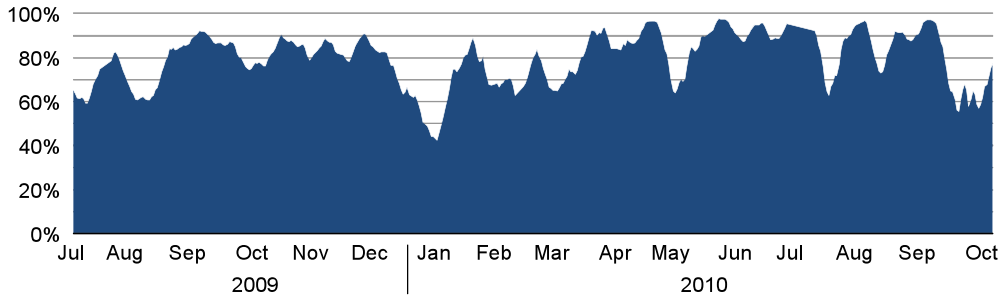


Figure 8 Spam from botnets

- As can be seen in Figure 8, there is often a decline in the proportion of spam sent from botnets at the end of the year. There may be many reasons for this, but the most recent is the closure of the Spamit affiliate program in late September 2010. Until then, Spamit was the largest known spam affiliate, mostly responsible for pharmaceutical spam for the Canadian Pharmacy brand. The largest botnets send mostly pharmaceutical spam.
- The top three botnets have not changed in the latter half of 2010. Rustock remains the most dominant botnet, with its spam output more than doubled since last year, to over 44 billion spam emails per day, with over one million bots under its control. Grum is second and Cutwail is the third largest.
- 2010 has seen a large increase in the volume of malware being sent in spam emails from botnet infected machines. Cutwail is the botnet most responsible for this, with massive volumes of Bredolab Trojan-infected emails sent throughout August. Grum has also been sending a variety of malware-infected emails throughout the year.
- The amount of spam coming from the US increased during the first half of 2010, accounting for over 10% of all spam by June. In the second half of the year this returned to 8.7%, similar to the level at the end of 2009.
- Spam from India has also increased in 2010, making it the largest single source of spam from one country, at 8.5% of global botnet spam.
- Spam from the Russian federation dropped from 9% of global spam at the end of 2009, to just over 3% in June. At the end of 2010, its output has risen to approximately 5% of global botnet spam.

Rustock

- Rustock remains the most dominant botnet and has been all year (peaking at just over 80% of all spam in mid-August). There was an observable dip in early October when the Spamit affiliate closed down; pharmaceutical spam accounted for the vast majority of Rustock's output. Since Spamit ceased operating, Rustock has had periods where very little or even no spam was sent from its bots. However, these outages were always short-lived (the longest being less than 48 hours). Even taking the outages into account, Rustock is still by far the most dominant spam-sending botnet.

- The US remains the main source of infection for Rustock, but it seems to have moved some operations away from bots in Europe and instead the second and third largest sources of infection are now in Brazil and India.

Grum

- The Grum botnet was positioned second in the list of most active spam-sending botnets at the end of 2010, accounting for approximately 9% of botnet spam, down from 16% at the end of the first half of 2010. Grum has not experienced any major outages in 2010 and has remained fairly consistent throughout the year, with output only falling at the end of the year.
- The number of active bots was down by more than 50% since the end of the first half of 2010, to between 310,000 and 470,000 bots worldwide.

Cutwail

- Like the Grum botnet, Cutwail has maintained its position in the top ten, remaining in third position, responsible for approximately 6% of global spam.
- Despite several takedown attempts during 2010, no action has managed to do more than marginally reduce the spam output from Cutwail for a brief period. Each time it has returned to business-as-usual within a day or two at most.
- The number of active bots has increased by approximately 16%, compared with the number of bots under its control at the end of 2009.
- During 2010, Cutwail has been the largest source of spam emails containing the Bredolab Trojan, and has been used to send the widest variety of spam across all the major botnets.

Maazben

- Maazben has not appeared in the top ten most active spam sending botnets since March 2010, when it was responsible for 0.4% of global spam. By the end of the first half of 2010, it had dropped out of the top ten altogether. By the end of 2010, it had moved up to fourth position, responsible for over 5.2% of global spam.
- The number of active bots under Maazben's control has increased by more than 1,000% since March 2010, to between 510,000 and 770,000 bots worldwide.

Mega-D

- Toward the end of 2009, attempts to disrupt the Mega-D botnet seemed to effectively eliminate it from the spam-sending landscape for several days. However, after only a few days it returned much stronger, using a larger number of brand new IP addresses from which it was sending spam. At that point it was responsible for almost 18% of global spam, but by the end of 2010, it has fallen to 2.3%.
- During 2010, the number of active Mega-D bots has dropped by around 58%.
- The spam output from each Mega-D bot has roughly halved every three months during 2010. In March, Mega-D sent approximately 428 spam emails from each active bot every minute; by the end of the year, the output fell to 105 spam emails per bot per minute.

3.2.3 Notable Botnet Changes

By the end of 2010 spam output from both Grum and Mega-D was down and both botnets had fewer active bots with a decline in output per bot per minute. This is likely due to a decrease in the number of bots under their control and perhaps by dropping their throughput, they are hoping to reduce the chance of others being discovered. It is also likely that they were reliant on a lot of business from the "Spamit" affiliate and have also suffered since its closure in October.

Cimbot is a botnet that has been around since at least March 2009, but in the past has never been particularly active. This is the first time it has ever made it into the top ten spam-sending botnets, and it may be the last time too as at the time of writing it had gone quiet again. Maazben has been around since August 2009 and has consistently appeared among the top ten botnets since, although it appeared to suffer a drop in size and output between March and June 2010, but has since returned to roughly the same as before.

Since its demise in 2008, the Storm botnet has been a minor botnet and has not contributed much to the overall spam landscape since. However, in April and May 2010 it made a significant reappearance and it was linked to a spam campaign making heavy use of legitimate shortened URLs that would redirect visitors to their spam web sites. Spam with shortened hyperlinks reached a peak of 18% on April 30, equivalent to roughly 23.4 billion spam emails. The Storm botnet first appeared in 2006 before declining in 2008, and in May spam from Storm accounted for 11.8% of all the spam containing shortened hyperlinks.

Asprox has been a relatively small botnet since it was severely disrupted following the closure of the McColo ISP at the end of 2008. In June 2010 it had a period where it dramatically increased the output from each bot, pushing it into the top ten for that period. However, that kind of output is not something any botnet has sustained for anything other than a short period, as it would greatly increase the risk of the bots being detected and cleaned up.

Since its discovery on December 31, 2009, the Lethic botnet is also still around, but has been in hibernation during September and the first half of October. It has since returned to previous levels and at the end of 2010 was responsible for as much as 3% of all spam. At the end of 2009, spam from Lethic accounted for 2.5% of all spam. Within 24 hours, spam from this new botnet increased to just under 4% and continued roughly at around that level for the following week, when it peaked at 5.25% of all spam. Its spam traffic then dropped off to almost nothing; disappearing almost as quickly as it arrived.

Like so much of the spam sent from botnets, the spam Lethic sent was roughly an even mix of pharmaceutical (all linked to the ubiquitous Canadian Pharmacy spam web sites) and some spam for replica watches. Furthermore, the Bagle sent exactly the same spam as the new Lethic botnet over the same time period. The templates for the pharmaceutical and watch spam were identical across both botnets and included hyperlinks to the same spam web sites.

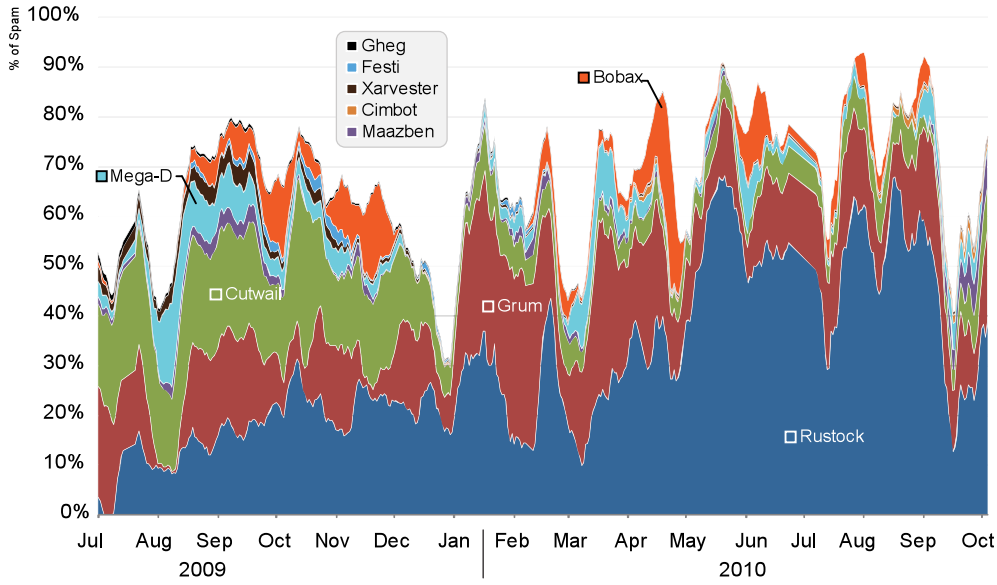


Figure 9 Spam from botnets

3.2.4 Rustock – The Rise and Fall of TLS[3] Encrypted Spam

Overall, the total amount of global spam in circulation decreased toward the end of 2010, with many botnets reducing their output. There were some exceptions however, particularly with Rustock, which continued to dominate and was responsible for 47.5% of all spam at the end of the year. To compensate for its shrinking size, Rustock had more than doubled the volume of spam sent from each bot per minute. This has resulted in Rustock pumping out more than 44 billion spams per day by the end of 2010, compared with 20 billion at the end of 2009, when it accounted for 19% of all spam.

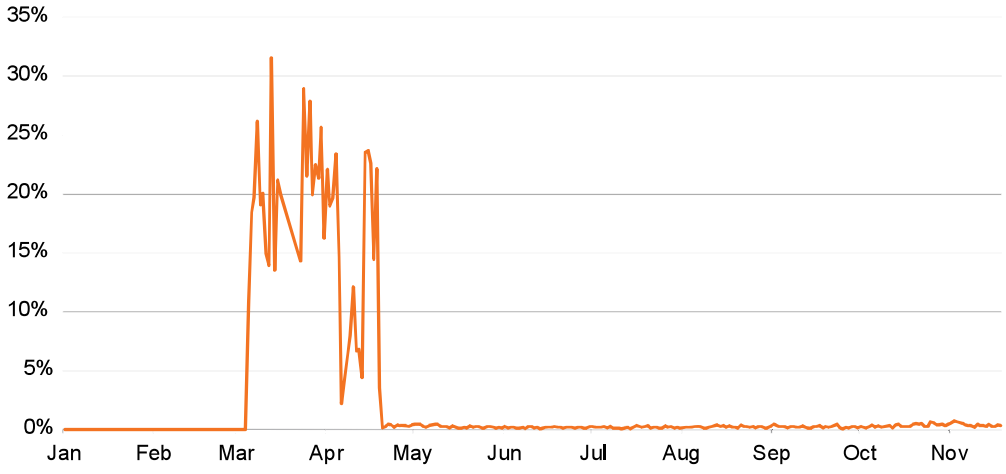


Figure 10 Spam sent using TLS

One of the factors in this increased throughput is that the Rustock botnet stopped using TLS encryption to send its spam, thus speeding-up its email connections. At its peak, in March 2010, TLS encrypted spam accounted for more than 30% of all spam and as much as 70% of the spam from Rustock was sent using TLS-

[3] *TLS – Transport Layer Security*

encrypted connections. However, since April 20, the use of TLS in spam-sending has fallen away and now accounts for between 0.1% and 0.2% of spam.

The use of TLS slows down a connection due to the additional encryption processing required and Rustock needed to recover this additional capacity to compensate for the recent contraction of the botnet in terms of its overall size. By turning off TLS, Rustock has been able to send more spam using fewer bots, than it had previously with more bots and by using TLS.

3.3 How Events and News Shaped the Spam Landscape in 2010

Spammers and scammers produce spam campaigns relating to most major newsworthy events. While the particular events may only have national or regional appeal, the approaches that spammers and scammers use are often similar.

3.3.1 FIFA World Cup

Major sporting events like the FIFA World Cup, which took place in South Africa in June 2010, are almost always exploited by spammers.

Before, during and after the event, MessageLabs Intelligence identified a wide variety of different threats relating to the FIFA World Cup, including spam, scams and advance-fee “419” fraud, and malware attacks.

The typical examples of fraudulent 419-style scam emails were offers for game tickets and fake hotel rooms. Some others included contract offers to supply clothing and boots, or offers for free mobile telephones. Some of the scams were a little more unusual, such as one that sought companies to provide additional electricity and power for the World Cup event itself. Ultimately, all of these scams were designed to obtain the recipient’s personal details and money by means of deception and fraud.

At the time, fake event tickets were also appearing for sale on a number of well-known auction web sites, which in reality were unlikely to be genuine and were contrary to the terms and conditions of use.

3.3.2 Spammers Harvesting News Headlines

Much of the spam related to the World Cup was not actually about the World Cup itself, but instead often spam advertising male enhancement products that included a random subject related to the World Cup event. In 2010, spammers were known to be able to automatically harvest headlines from hundreds of web sites, including news web sites and blogs, and to use these in their subject lines. This approach enables the spammers to collect topical themes and insert them into their messages, often as “Bayes” poison hidden within the body of the spam message, in an attempt to make each message unique and confuse some of the more basic spam detection techniques.

The World Cup theme was also used as bait in a number of malicious emails, one example of which can be seen in Figure 11. The email was composed in Portuguese and contained the branding of one of the major sponsors of the forthcoming competition.

Figure 11 World Cup spam example

Further analysis identified that although the email attempted to spoof a well-known US soft drink brand, it had actually been sent from an IP address in Macau.

Figure 12 World Cup malware example

The malware, if activated, would collect information about what other machines were on the same network, steal data and enable a remote attacker further access to the compromised computer.

Cyber criminals also used the World Cup as a theme to disguise targeted attacks[4]. Targeted attacks are arguably the most damaging internet threat.

3.4 A Review of Significant Spam Tactics in 2010

3.4.1 Spam Message Size

Throughout the year, over 72% of all spam was less than 5kB in size. This makes sense from a spammer's point of view as less data sent per message means many more messages can be sent and more potential victims reached. Small file sizes are achieved by keeping the message short and simple, often just including one line of text and a link to a web page. As well as allowing greater volumes to be sent, shorter messages are more likely to be read than long ones.

---

[4] *For more information, please read the following blog posts:*

http://www.symantec.com/connect/blogs/targeted-attack-uses-fifa-world-cup-2010-hook; http://www.symantec.com/connect/blogs/fifa-world-cup-used-lure-victims-targeted-attack; http://www.symantec.com/connect/blogs/brazilian-world-cup-related-targeted-attack

Despite most mails being less than 5kB, if we look at the average size day to day since the start of this year, we can see some noticeable increases in the average size, particularly through April to June, and again in August.

Throughout April, May and June, the increase in average file size was due to a long run of HTML format emails (with some attached images) being sent by both the Rustock and Cutwail botnets. Mostly this was the common "pharmaceutical" spam, with some replica watch spam as well.

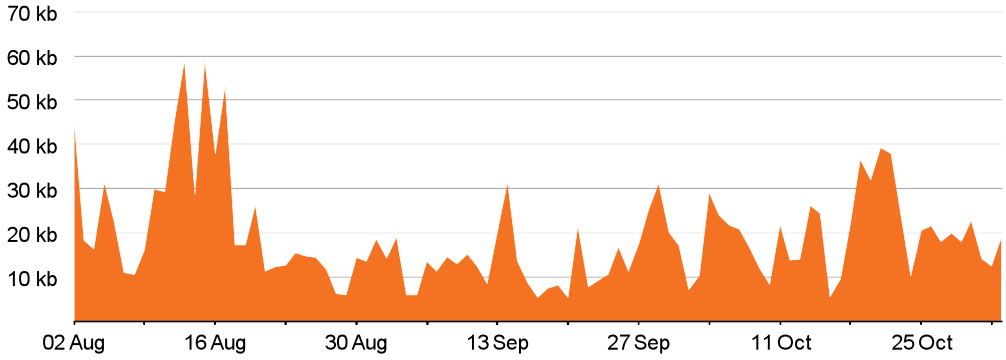


Figure 13 Average size of spam email over time

However, the rise in August was different; while it was Cutwail again that was responsible for the increase, it was not image spam this time. Throughout August, the number of compressed archives being sent in spam increased dramatically.[5]

3.4.2 Shortcuts for Spammers – Increased Use of URL Shortening Services in Spam Emails

During 2009, with the explosion of social networking and micro-blogging services, the use of URL shortening services became more popular. Many such services do not require users to register or complete a CAPTCHA[6] to use their services. This tactic was reported in detail by MessageLabs Intelligence in its 2009 Annual Report[7], but over the last quarter the volume of spam that contains such links has increased significantly.

The spammers' use of URLs from link shortening services became increasingly popular during 2010. At its peak, on July 28, 2009, 9.3% of spam comprised some form of shortened hyperlink provided by one of the many free online shortening services, equivalent to more than 10 billion spam emails each day, worldwide. On April 30, 2010, this peak figure had almost doubled to 18.0% of spam, the current historical peak.

---

[5] *See section 4.4 for more detail on compressed archives*

[6] *CAPTCHA – Completely Automated Public Turing test to tell Computers and Humans Apart*

[7] 2009 MessageLabs Intelligence Annual Report *http://www.messagelabs.com/mlireport/2009MLIAnnualReport_Final_PrintResolution.pdf*

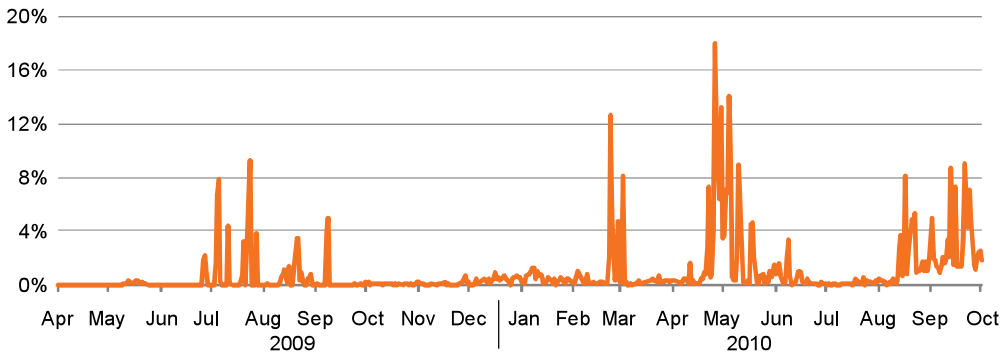


Figure 14 Percentage of spam containing a short URL

MessageLabs Intelligence has seen a steady rise in the average percentage of spam containing a shortened URL since mid to late August. The botnets responsible for this sustained rise in the baseline proportion of spam that uses short URLs, were Cutwail and Grum, which suddenly started pumping out lots of pharmaceutical and replica watch spam containing shortened URLs; much more than they had done during previous months.

Since mid to late August, at least 1% of spam each day has contained a shortened URL. For September 2010, the proportion of spam that contained a shortened URL reached 3% of spam for the month and to date this figure has been tracking at approximately 2% of all spam.

Since August 2010, rather than shortened URLs being used in large waves of spam, their use has become much more steady, with no significant peaks since May 2010.

Top 10 short URLs used in spam 2009	
bit.ly	12.0%
o.ly	8.5%
su.pr	8.1%
aafter.us	7.9%
tcbp.net	7.6%
jtty.com	5.8%
tlink.me	5.7%
myurl.in	5.2%
snurl.com	4.9%
Other	34.3%

Top 10 short URLs used in spam 2010	
bit.ly	10.4%
su.pr	6.0%
kl.am*	3.6%
doiop.com*	3.6%
ho.io*	2.7%
snurl.com, livefilestore.com	2.6%
snipurl.com*	2.5%
snipr.com*	2.5%
retwt.me*	2.3%
Other	63.8%

*new to Top 10 in 2010

Figure 15 Top short URL service used in spam 2009 vs. 2010

On average, 91% of spam contained some kind of URL in 2009 and in 2010 this is almost unchanged at 91.1%. An average 0.33% of all spam contained a short URL in 2009, and in 2010 this figure rose to 1.38% (1 in 72.5), with an average of 1 in 66.1 of all URLs in spam being shortened in 2010.

3.4.3 Tracking Response Rates for Shortened URL Services

One of the most frequently seen short URL services in spam is the “bit.ly” service. Bit.ly also provides a service whereby users can view statistics on a given shortened URL by appending a ‘+’ after the short URL e.g. http://bit.ly/mli2011a+

MessageLabs Intelligence can collect all of the statistics from these pages and analyze the click-through responses for shortened URLs using this provider. Most of

the bit.ly shortened URLs were used for pharmaceutical products and watches. Approximately 21.2% of shortened URL spam contained links to bit.ly URLs, generating approximately 27.2 responses for each spam email that contained a bit.ly URL, and 44.2 responses per bit.ly URL.

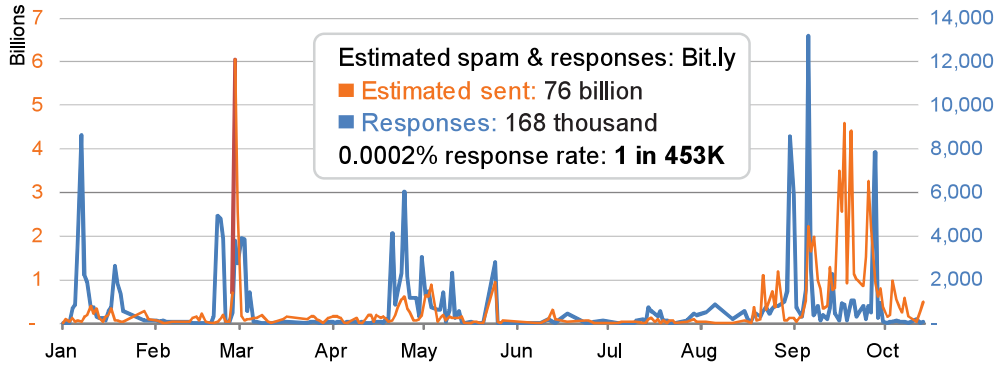


Figure 16 Estimated spam and responses to spam with a bit.ly shortened URL

In Figure 16 it can be seen that responses to bit.ly shortened URLs peaked at 13,225 in a single day on September 5, 2010.

If we take a closer look at the campaign responsible for this, it was a single URL (http://bit.ly/ch[obfuscated]) that first appeared in spam on September 4, 2010. In total MessageLabs Intelligence estimates that 352 million spam emails were sent globally over a three day period. The shortened URL generated a total of 18,437 responses.

The URL is redirected to a replica watch web site.

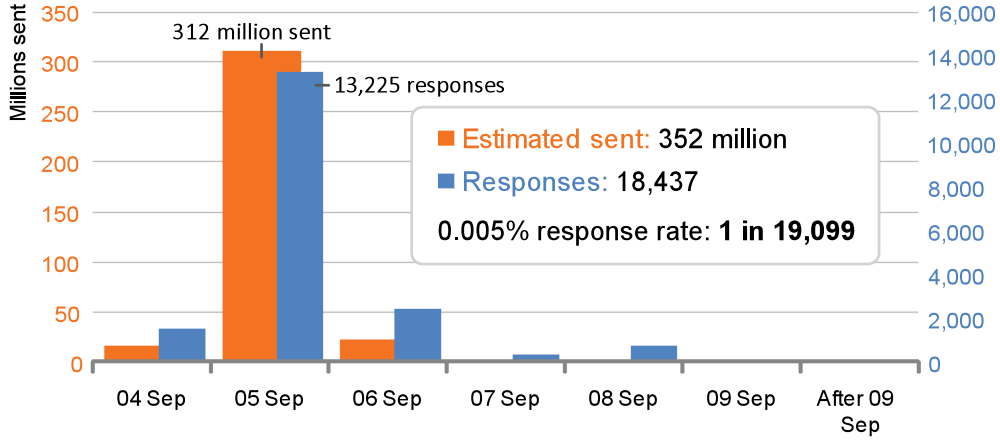


Figure 17 Estimated spam and responses to a single selected spam run

From this analysis we can see that responses are generated at a rate which is slightly slower than the rate at which the spam is being sent, presumably because spam is likely to sit in recipients' inboxes for possibly many hours before being opened, depending on the various time zones involved.

After three days, the campaign using this specific short URL ended. After the spam campaign had finished, 93.5% of the responses were already in, with responses still trickling in more than one month later.

This is an important factor, as it shows that spammers do not need to hang around to wait for responses. In this case bit.ly was still allowing requests to this shortened URL, but in other examples the shortened URL may have been removed after a few days and can become unavailable very quickly. It is therefore in the spammers'

best interests to establish the shortened URLs, and distribute the spam emails as quickly as possible to capture the maximum responses in the shortest possible time, before moving on.

In this particular example, the spammers did rather well and attracted 18,437 responses within just three days of spamming. How this translates into financial commission is difficult to ascertain, but it is likely that their income would have been generated from an affiliate scheme relating to the fake watch web site.

3.4.4 Spammers Get Creative

Spammers will try anything to get their spam past anti-spam filters, including tricks involving random text hidden in the body of the messages, images and message bodies with nothing but a URL to the main message located elsewhere on the web. Figure 18 is an example of the more elaborate attempts that were tracked recently.

MessageLabs Intelligence identified a run of emails that pretended to inform the recipient that they had a number of “unread” or “important” messages waiting for them on a well-known social networking web site. Over a three day period, between 24 and 26 October 2010, roughly 18,500 of these emails were blocked, before falling to approximately 100 per day.

The use of a well-known social media brand name is the first part of the approach to bypass filters; the message copies the format of commonly used email subjects, making it harder to rely on signature-based detection in relation to the subject alone. It is also useful as a social engineering technique, to try to entice an unsuspecting user into opening the email.

Upon opening the email, it is clear that despite the subject, it has nothing to do with the social network mentioned in the subject line, but is instead spam trying to get people to buy pharmaceuticals

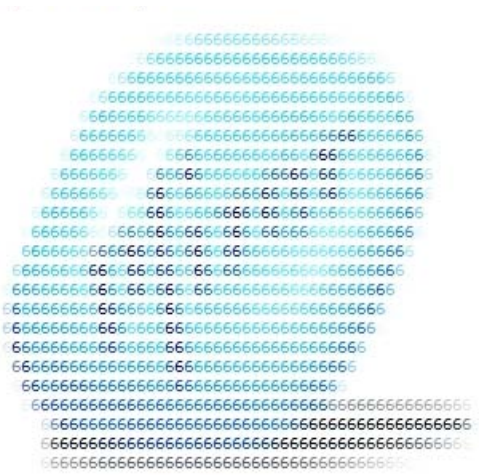
Figure 18 Spam appearing to contain images

At first glance this looks like image spam, where the text is actually part of an image in an attempt to make it readable by humans but not computers. However, in this case there are no images in the email. If we look at the email with HTML rendering turned off, the plain text section displays a list of URLs for genuine companies, perhaps in an attempt to fool anti-spam filters. This is then followed by some seemingly random text.

Figure 19 Email with body highlighted to reveal all text

However, the text is not random at all, but is instead intended to disguise the real text of the email by making it much harder to automatically recognize certain words.

The use of HTML tags to change background and font colors allows the spammers to make only the desired characters visible to humans. To a machine, it still appears as simple text in HTML format, thus making it very difficult for standard filters to spot certain words. In this case the use of HTML also makes what appears to be a green cross image, commonly used in many countries to signify a pharmacy.



Similarly, over the years, "ASCII art" - or the use of the ASCII character set to produce a picture - has been used sporadically in spam. Spammers use it as a way to obfuscate words, presenting messages written in ASCII art rather than simple text. This often frustrates attempts by some of the more basic anti-spam technology to recognize certain phrases.

More recently though, in 2010, spammers have adapted[8] their approach and used software to render an image into ASCII text, for example, taking a picture of a blue pill and turning it into HTML that displays the image in a web browser or an email client as colorful ASCII art, such as in the example in Figure 20.

3.5 Web-based Email Services and Spam

Spam originating from webmail services is not as common as it once was; only 0.7% of spam in 2010 was sent from a webmail account. This is because most spam is now sent from botnet-infected computers, and the major spam-sending botnets do not tend to use webmail services. What was slightly more common, however, were spam emails that pretended to be sent from webmail accounts; 1.1% of spam had a forged "From:" address designed to appear as if it had been sent by a legitimate webmail account.

---

[8] *For more details, please read this blog post: http://www.symantec.com/connect/blogs/spammers-get-creative-ascii*

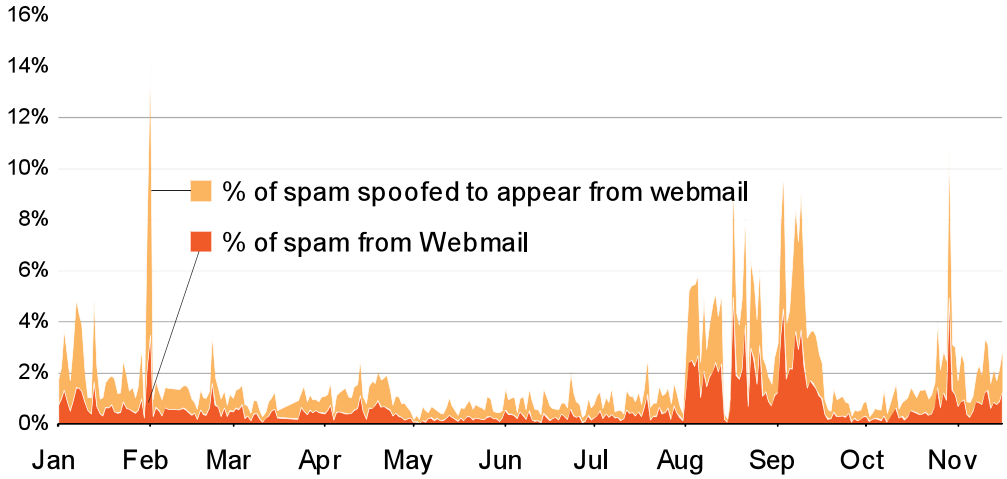


Figure 21Spam from webmail services and spoofing webmail services

The increase noted during August was the result of an increase in spam from a single unidentified botnet and an increase in spam from the Donbot and Cutwail botnets. Much of the spam in this period from the unidentified botnet was very similar to spam we know to have come from Donbot, and it was suspected that it may have been a variant of the Donbot botnet.

Although botnets do not generally send much spam from genuine webmail accounts, 89% of spam that is sent from webmail accounts does originate from botnets. Most of it is from small, unidentified botnets. Some of these may be known botnets that may not be recognized as such because of the different approaches used to send spam; for example the typical SMTP conversation patterns associated with a particular botnet may not be recognized as the same when sent through a well-known webmail provider. Some webmail providers do not include the IP address of the original sender, so the only IP addresses included in the message headers are for the webmail provider, and MessageLabs Intelligence is unable to then match the sender IP against known bots.

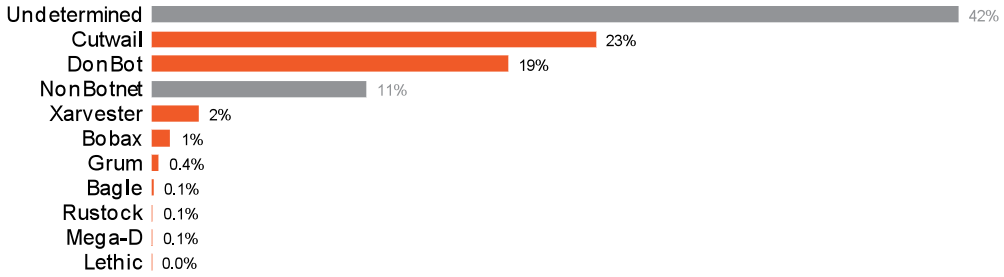


Figure 22 Source of webmail or spoofed webmail by botnet

Figure 22 highlights the fact that botnet controllers will use any tools at their disposal, including utilizing webmail accounts – by either hijacking a legitimate user account or using automated CAPTCHA breaking tools. However, most spam is still sent directly from infected botnet computers; webmail providers will throttle-down unusually high volumes of email from individual accounts and may even suspend the accounts for violating terms and conditions.

3.6 Classification of Spam Categories

3.6.1 The Challenge of Categorization

It is not always straightforward to classify spam into particular categories; spam comes in a variety of different styles and complexities. Some spam is plain text with a URL; some is cluttered with images and attachments. Some arrives with very little text and perhaps only a URL. Spam also comes in a variety of different languages, most commonly English, but other common languages include: French, Russian, German, Spanish, Chinese, and Portuguese. It is also very common for spam to contain "Bayes poison," which is random text added by spammers often harvested from web sites to litter the spam with a large number of words that bear no relation to the theme of the spam.

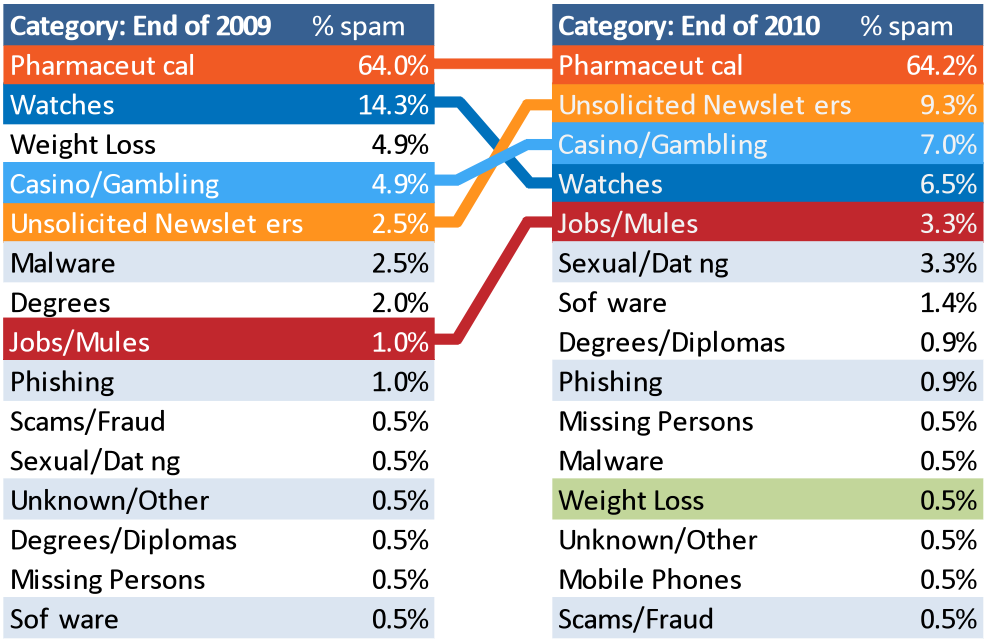
Spam emails are meant to be read by humans, and so often the spammer's priority is to get their message to the recipient, without giving away the theme in the email's plain text, which is examined by automated anti-spam techniques.

Since spam is obfuscated to avoid automated detection it is necessary to manually review a large sample of spam to develop an accurate sense of the trends in categories. Just like the intended recipient of a spam email, an analyst can read the message to get a sense of the context of the email, and then view any images in context together with the message in the email and by following hyperlinks. It is time-consuming but it gives much more accurate results.

3.6.2 The Dominance of Pharmaceutical Spam

Approximately two-thirds of all spam is related to pharmaceutical products, and historically a great deal of that is related to Canadian Pharmacy web sites and related brands. It is an enormous money making machine in the shadow economy, and spammers would line up to work with affiliate schemes such as Spamit, distributing enormous volumes of rapidly changing spam and taking commission for their efforts.

In October 2010 Spamit was closed but MessageLabs Intelligence did not see a drop in "Canadian Pharmacy" spam once again showing the resilience of these criminal enterprises.



Category: End of 2009	% spam
Pharmaceut cal	64.0%
Watches	14.3%
Weight Loss	4.9%
Casino/Gambling	4.9%
Unsolicited Newslet ers	2.5%
Malware	2.5%
Degrees	2.0%
Jobs/Mules	1.0%
Phishing	1.0%
Scams/Fraud	0.5%
Sexual/Dat ng	0.5%
Unknown/Other	0.5%
Degrees/Diplomas	0.5%
Missing Persons	0.5%
Sof ware	0.5%

Category: End of 2010	% spam
Pharmaceut cal	64.2%
Unsolicited Newslet ers	9.3%
Casino/Gambling	7.0%
Watches	6.5%
Jobs/Mules	3.3%
Sexual/Dat ng	3.3%
Sof ware	1.4%
Degrees/Diplomas	0.9%
Phishing	0.9%
Missing Persons	0.5%
Malware	0.5%
Weight Loss	0.5%
Unknown/Other	0.5%
Mobile Phones	0.5%
Scams/Fraud	0.5%

Figure 23 Spam categories at the end of 2009 vs. end of 2010

While pharmaceutical spam dominates categories, even 0.5% of spam volume represents a huge number of spam messages if you consider that there are an estimated 130.5 billion spam messages sent per day.

For most of 2010, Rustock, the largest spam-sending botnet, has been responsible for most of the pharmaceutical spam in circulation. Throughout 2010, the proportion of spam that was pharmaceutical in nature didn't drop below 64%, comparable with 2009. However, the closure of the spam affiliate, Spamit, is likely to have provided a setback for some spam gangs.

- ***Pharmaceutical:*** The aim of most pharmaceutical spam is to encourage recipients to click on a link in the email that leads them to a web site selling a variety of pharmaceutical products such as pills/drugs for anything from male enhancement, to weight loss, to stress relief. Over the last year up to 85% of spam has been related to pharmaceutical products. Currently it accounts for about two thirds of all spam. Considering that an estimated 130.5 billion spam emails are in circulation globally every day, the contribution from pharmaceutical spam equates to 80 billion messages being sent to unfortunate recipients all over the world each day.
- ***Watches and Fake Designer Goods:*** Ads for fake designer goods including watches have always been common in spam, especially in the build-up to Christmas and the New Year. There is always some watch spam around, but seldom challenging the volumes of spam related to pharmaceutical products. Watch spam was more common in 2009 at 14.3%, and mostly sent from the Donbot and Cutwail botnets.
- ***Unsolicited Newsletters:*** The second most common type of spam in 2010 was unsolicited newsletters. These have been around for many years and recipient email addresses are collected by a number of methods. Most unsolicited newsletters were sent from the Xarvester and Mega-D botnets.
- **Casino/Gambling Spam:** Casino spam, like watch spam, is always around, but only occasionally does it account for a significant proportion of spam. At the end of 2009, it accounted for 4.9% of spam, but in 2010 it has averaged around

3.3%, rising to 7% by the end of the year. Casino spam is commonly written in both English and German.

- **Sexual/Dating Spam:** Sexual/dating spam has become much more common in 2010. These are emails containing pornographic images, or links to pornographic or dating web sites. At the end of 2009, sexual/dating spam accounted for 0.5% of spam. During August, September and October 2010 it has increased to as much as 5.6% of spam at its peak, when much of it was being sent from the Cutwail and Mega-D botnets.

3.7 Languages of Spam

To determine the language in which an email is written, it is first necessary to ignore the email headers. MessageLabs Intelligence then runs several different language recognition modules over the body text, each module being better at recognizing some languages than others, before arriving at a decision as to which is the most likely language based on the combined results of each module.

In January, 96% of spam was in English, but this has declined very slowly over the year until falling to an all-time low at 90% in August, where it has remained since.

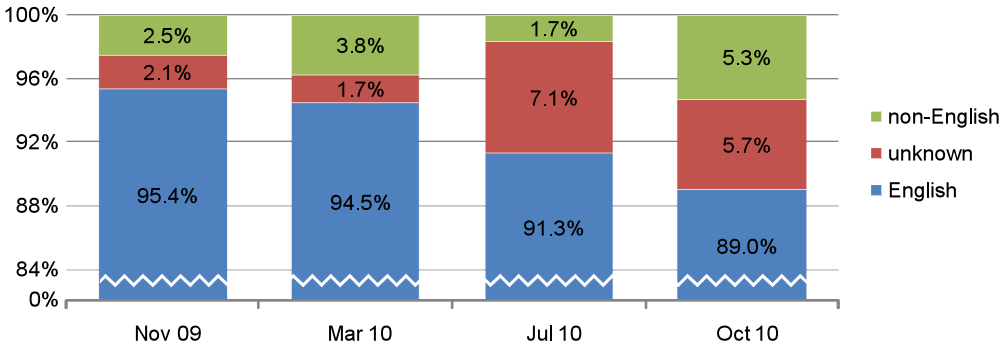


Figure 24 Spam in English, other languages or unknown

So what makes up the non-English spam? About half of it is classified as “unknown” and this often means that there is not enough recognizable text within the body of the email to be able to determine a language. In most cases this is because the body only contains a very small amount of HTML code, such as a hyperlink to a web page or an image. Since January, the amount of unknown language spam has been steadily increasing in line with the decrease of English language spam. This is likely due to an increase in remote image spam, where the body of the email itself contains only enough HTML to display a remotely hosted image. The mail body does not need to contain much text, as anything the spammer wants to say can be included in the remote image

Language	% of all spam
Dutch	1.3%
French	1.0%
Russian	0.9%
Spanish	0.7%
German	0.5%
Chinese	0.5%
Portuguese	0.2%
Japanese	0.1%

October 2010

Table 4 Non-English spam

The remainder of the non-English spam is in many languages and since January 2010, the second most popular language in spam has been Dutch.

It is difficult to ascertain whether spam in languages other than English is increasing overall, since the volumes are relatively low when compared with English-language

spam; any variations observed are more likely to be a result of English or unknown language spam changing in volume.

3.8 Botnets and Spam Languages

We already know that most of the spam in circulation is sent from botnets. So are there any particular botnets that are responsible for spam in languages other than English? Five of the top botnets are Rustock, Grum, Mega-D, Maazben, and Cutwail; among them, these botnets are responsible for over 90% of all spam.

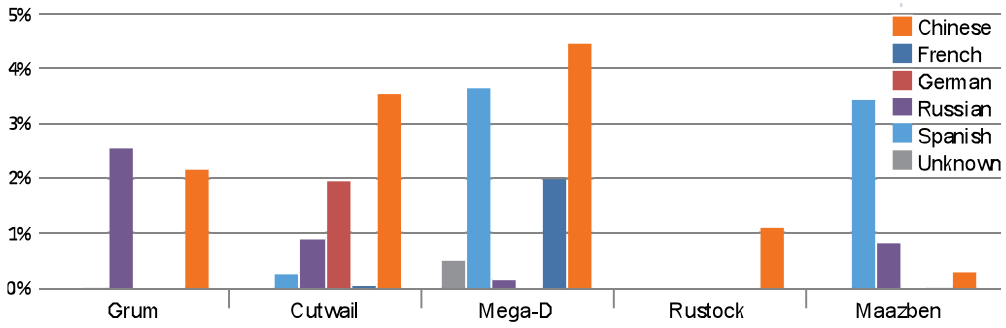


Figure 25 Botnet sources of non-English spam

Of these botnets, Mega-D is the most multilingual, with 6.4% of its traffic in languages other than English, and a further 4.5% classified as unknown language. Mega-D sends Chinese (0.6%), French (3.7%) and Spanish (2.0%) language spam, all of which are disguised as job advertisements, offering ways to earn large amounts of money for little effort. In reality, it is likely that the spammers are just after personal details, or are trying to start a money mule-type scam which will take money from the victim.

For Rustock, the largest of the botnets, we have seen no spam in languages other than English. In fact, 98.9% of its spam can be classified as English, with the remaining 1.1% classified as unknown. As Rustock is the largest source of global spam, it is a large part of the reason there is so little spam in languages other than English.

3.8.1 Language of Spam Received in Various Countries

English is the most common spam language received in every country except Brazil. Brazil is the only country examined where the most common language is neither “unknown” nor English. Approximately 33% of spam sent to Brazilian recipients was in Portuguese. Brazil has one of the lowest percentages of English language spam at 25.6%.

Rank	Country	Local Language(s)	% in Local Language	Rank	Country	Local Language(s)	% in Local Language
1	Brazil	Portuguese	32.8%	14	Austria	German	8.3%
2	Ecuador	Spanish	27.0%	15	Denmark	Danish	4.0%
3	Mexico	Spanish	25.5%	16	Bermuda	Portuguese	2.3%
4	Portugal	Portuguese	22.7%	17	Israel	Hebrew/Arabic	2.1%
5	Spain	Spanish	20.6%	18	Netherlands	Dutch	2.1%
6	Italy	Italian	19.1%	19	UAE	Arabic	2.0%
7	France	French	13.9%	20	Bahrain	Arabic	2.0%
8	China	Chinese	13.4%	21	Sweden	Swedish	1.6%
9	Switzerland	French/German/Italian	12.1%	22	Kuwait	Arabic	1.3%
10	Belgium	French/Dutch/German	11.0%	23	Hungary	Hungarian	0.6%
11	Saudi Arabia	Arabic	10.4%	24	Ireland	Irish	0.5%
12	Germany	German	9.6%	25	Finland	Finnish/Swedish	0.5%
13	Japan	Japanese	8.9%	26	Poland	Polish	0.2%

Table 5 Countries with high rates of local language spam

We have seen that Portuguese and Spanish are some of the most popular languages used in spam. In Portuguese and Spanish speaking countries, the local language element is high.

The proportion of spam that is in the local language in each country is variable over time as cyber criminals modify tactics. A huge run of English spam will depress the percentage of spam received in other languages.

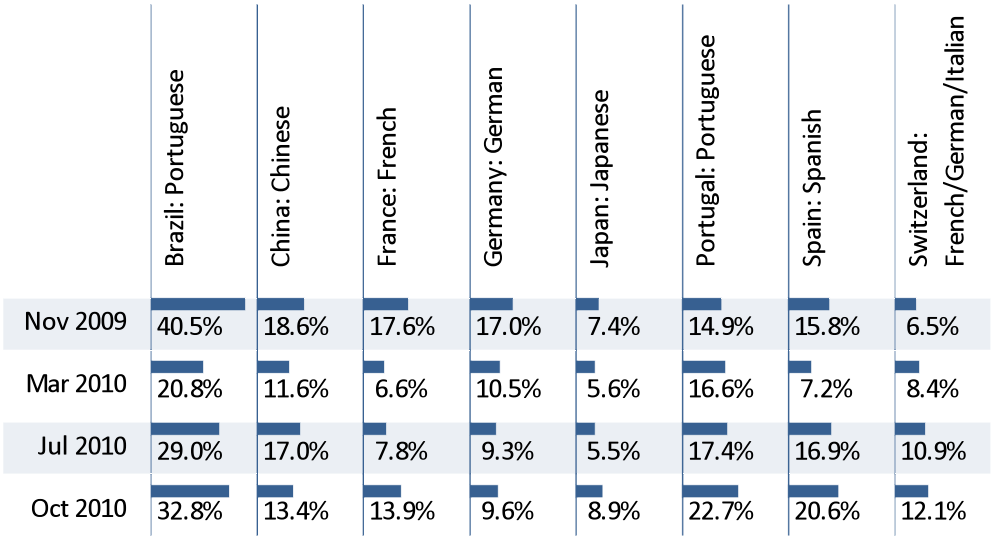


Figure 26 Country rates of spam in the primary language(s) of the country

In most countries, the percentage of spam in the local language took a dip at the beginning of the year and has since recovered or exceeds the percentage seen in November 2009.

Spanish spam has become more common, mainly because a couple of the major botnets have been pumping out Spanish spam during the last few months of 2010. Globally the amount of spam in German, Portuguese or Japanese has not increased. Japan, Portugal and Switzerland are receiving more spam in their local language, suggesting that spammers are making more of an effort to target particular countries in regions with the appropriate language.

Globally, the proportion of all English spam is decreasing. It appears the increase in spam in non-English languages is targeted to an appropriate country, which makes

sense as, for example, sending, Japanese spam to a primarily English, or German speaking country would be a waste of time.

3.9 File Types Found in Spam Messages

There are three categories of spam:

- Spam without links or attachments – no associated file
- Spam with links to a file or web page
- Spam with attachments

Between January and June 2010, most spam email contained a link to a file in it. Over those six months, 63% of email on average had a link to some kind of file or had a file attached to the mail itself. Since around June 12, however, this has declined to the point where there is now less mail that has a linked or attached file than there is without. In the time from June to October, only 44% of email contained a link to a file, or an attached file.

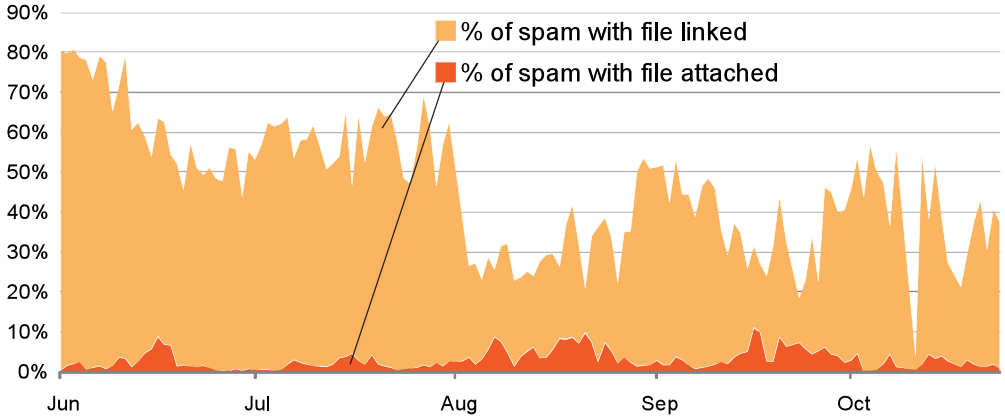


Figure 27 Spam with links and attached files

3.9.1 Hosted Files in Spam

Most of these files are not attached to the email; rather they are linked to in HTML.

- **Remotely Hosted Images:** Of these remote files, almost 70% are image files. Typically, these image files form part of an email written in HTML format, and are used either to make spam that looks like legitimate professional marketing spam (e.g. brand logos, product images), or to replace what would normally be a text body (so the image contains text) in an effort to evade text-based spam filtering.
- **Specific Web File Type Links:** After images, the next most common type of file linked to in spam email is web page files. This includes HTML files, PHP files, ASP files, etc. Normal marketing emails often contain links, but generally they link to a site (e.g. http://www.somesite.com/) rather than a specific file (e.g. http://www.somesite.com/sub/somefile.php). These tend to be used when the spammer wants their target to visit a specific section of a web site, which is often because the main site is used for purposes other than the subject of the spam. This could be a site that the spammers use for various unrelated spam runs, which each have their own unique pages. Or it could be that the spammers have compromised a legitimate web site and inserted their content. In this case, they could not give out a link to the main site as it would be obvious that it had nothing to do with the subject of the original spam.

- **Remotely Hosted Executables:** Other types of files that are linked to in emails are executables, compressed archives and documents. Links to these types of files are rare though, as they are usually attached to the email rather than hosted remotely. In total they account for only 0.14% of all linked files in spam since June 1. An exception to this is executable files which are more commonly found as links than attachments. This is because almost all email systems will now block executable files from being sent, as they could so easily be malicious. They are still rare in links as even though a remote executable file bypasses most email scanning, it would still be blocked by most web scanning software, so very few would ever reach their intended targets.

3.9.2 Attached Files in Spam

In 2010, it is much less common to see spam with files attached. Since June, only 3% of spam has had a file attached, with a peak of 11% for one day in September. The reason for this is mostly because of the difference in size between spam with attached files, and those with just a link. An email which has a file attached will always be bigger than one that contains a link to the file instead. This is important to spammers since the size of an email will have a direct effect on how many can be sent in a given time period. A bigger file size means less mail sent, less mail sent means less money for the spammers.

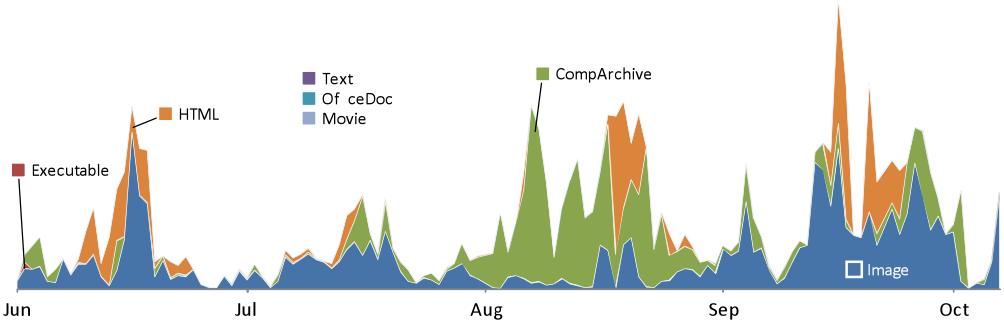


Figure 28 Attached file types in spam

- **Image Attachments:** Images are mostly used as a way of bypassing text-based spam filters, as recognizing text in images is a much more complicated process than a plain text file.
- **HTML File Attachments:** Rather than put the HTML in the body of the email, the spammers have sent it as an attachment. Most modern email clients that can render HTML will display the attachment so it still appears to be in the body.
- **Compressed Archives:** These are used as a way of disguising the true payload. This is because it is impossible to tell what is in an archive file just by looking at it -- it must be opened. To compound the issue, archive files can be encrypted and password protected, making it impossible to view the contents unless you have the password. When being used in spam, the password must be in the email or the intended victim would not be able to get to the payload. There are many ways of adding a password to an email that are easily readable by a human, yet extremely difficult for a computer. Another reason for using compressed archives to deliver payloads is simply that it will reduce the overall size of the mail, and as discussed earlier, less size means more spam in a given time. For these reasons it is very rare to see uncompressed executable files or documents in spam.

4 MALWARE: TOP THREATS OF 2010

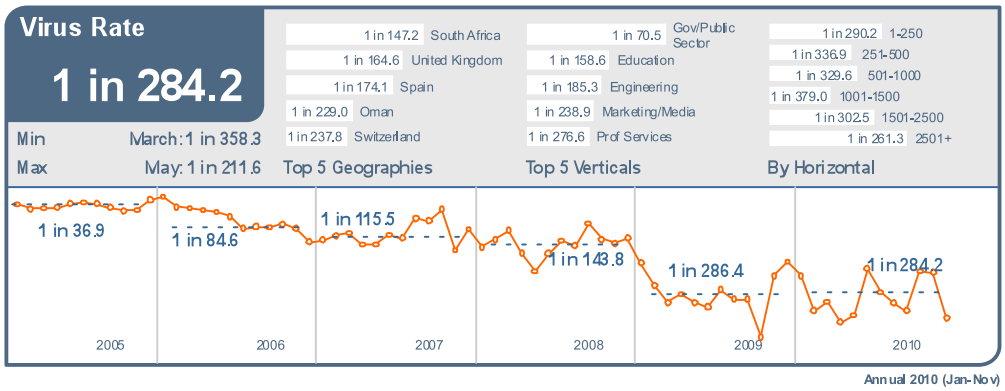


Figure 29 Virus rate

In 2010, the average rate for malware contained in email traffic was 1 in 284.2 emails (0.352%), almost unchanged when compared with 1 in 286.4 (%) for 2009. Approximately 23.7% of malware blocked in 2010 was contained in a malicious link within the body of the message, as opposed to an attachment. This compares to 15.1% of malware blocked contained in a link during 2009.

In 2010, over 115.6 million emails were blocked by Skeptic™ as malicious, representing an increase of 58.1% compared with 2009. There were 339,673 different malware strains identified in the malicious emails blocked. This represents more than a hundredfold increase over 2009 and is due to the growth in polymorphic malware variants. These are typically generated from toolkits that allow a new version of the code to be generated quickly and easily. An example of this includes the Bredolab family of Trojans, a general-purpose botnet linked with Pandex and Cutwail, which accounted for approximately 7.4% of all email-borne malware in 2010. There is more information about Bredolab later in this report.

There have been a number of notable developments in email-borne malware during 2010.

The **Stuxnet Trojan**[9] made tangible the potential for malware to materially impact industrial control systems hardware and cause significant disruption beyond cyberspace.

The September outbreak of the "**Here You Have**" virus (a.k.a. W32.IMSOLK.B@mm) demonstrated that even after 25 years, the signature-based approach of anti-virus countermeasures is still inadequate. With Skeptic™ and its 10 year pedigree as the pioneer of security in-the-cloud, Symantec was able to protect its MessageLabs clients against this attack. Clients of one of Symantec's cloud-based rivals were unprotected for over four hours by which time almost 90% of the threat had already passed.

Targeted attacks, also known as Advanced Persistent Threats, have the ultimate aim of gaining access to specific sensitive data, corporate intellectual property or access to confidential internal systems. This is undertaken by targeting specific

[9] *For more information on the history of Stuxnet, please read this blog post: http://www.symantec.com/connect/blogs/stuxnet-breakthrough*

individuals within specific companies. Targeted attack emails are sent in very low volumes, especially when compared with spam and phishing emails, but are potentially one of the most damaging threats any organization can face.

4.1 Botnets & Malware

4.1.1 Botnets and DDoS – Ten Years of Distributed Attacks

Botnets are extremely versatile and can be used for many functions in addition to sending huge volumes of spam each day. Botnets can be used to host bullet-proof web sites, and launch Distributed Denial-of-Service (DDoS) attacks against other services and businesses online.

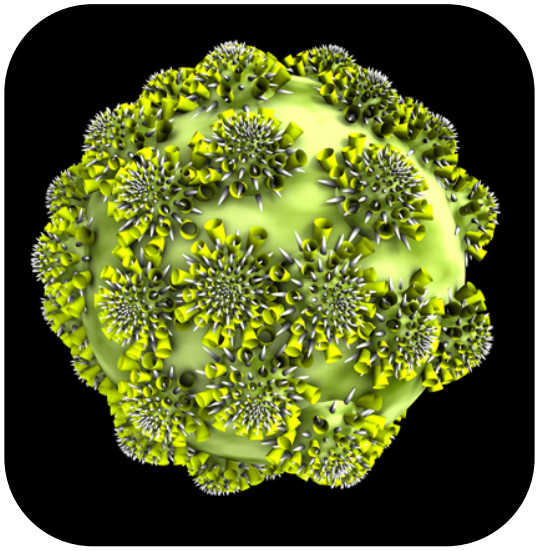
Ten years ago, on 14 February 2000, DDoS attacks – which attempt to cause disruption to an online service or application – knocked a number of high profile web sites offline for several hours, including a well-known auction web site, the web site of a global news channel and an internationally recognized online retail web site.

In 2010 we see DDoS attacks served up by huge botnets. DDoS attacks have evolved to be more sophisticated, more prevalent and more dangerous than ever.

There are concerns that in the future botnets will become increasingly self-sufficient which could make them even more efficient at propagating DDoS attacks. Following the 2008 takedown of McColo, a rogue ISP based in California, spam-sending botnets started to make a speedy recovery within a matter of weeks. Since McColo, botnets have changed; savvy botnet owners now have built-in business continuity plans to ensure their networks are self-sufficient, robust and less prone to disruption. Clearly, attackers have learned the importance of having a proper backup strategy for their command and control channels. Semi-automated networks mean that cyber criminals are now free to pursue new business opportunities while targeted DDoS attacks take down critical online applications and services on their own.

4.1.2 Ten Years On From LoveBug

On May 4, 2000 the MessageLabs Intelligence[10] team was the first to name the LoveBug virus, a mass-mailing worm that was first stopped by Skeptic™ at 00:14 a.m. (British Summer Time). It proved to be a historic day as virus levels surged overnight from one in every 1000 emails to one in 28. Launched from the Philippines, LoveBug started to wreak global damage as countries came online to begin their working day. Emails with the subject line 'ILOVEYOU' dropped into inboxes across the world. Ten years ago,



[10] *For more information, please read this blog post: http://www.symantec.com/connect/blogs/lovebug-virus-turns-ten*

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. Once opened, the attachment contained malicious VBScript that sent itself to every email address in the recipient's address book. LoveBug went on to affect 45 million computer users worldwide.

As a result of the LoveBug virus, legislation in the Philippines was changed and today some highly effective legislature exists to combat online crime.

Although the threat landscape is drastically different 10 years on, with attacks increasing in sophistication and engineering, it was perhaps surprising that later in 2010, an old-style virus outbreak similar in many ways to LoveBug was able to gain significant momentum – that virus was IMSOLK.B.

4.1.3 "Here You Have" IMSOLK.B: A Wake-up Call For Businesses

On September 9, 2010 at 15:20 (GMT) Skeptic™ identified a new virus attack which used old mass-mailer techniques. Using Skeptic™'s unique predictive heuristics, it was blocked before it reached any clients' networks. The heuristic rule that triggered the detection of this virus by Skeptic™ was actually added in May 2008.

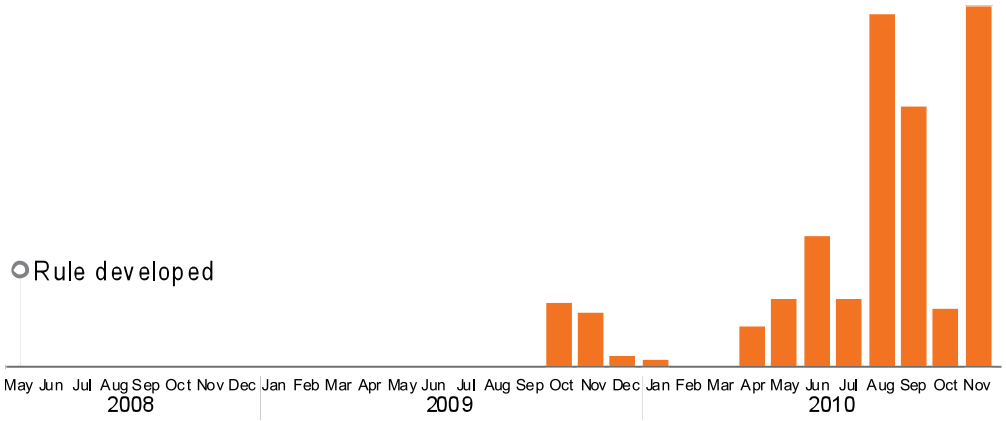


Figure 31 History of Skeptic™ heuristic rule that stopped Imsolk.B trigger events

At its peak, over 2,000 malicious emails were blocked per minute. The last copy was blocked on September 10, 2010 at 08:33 GMT, during which time 106,390 copies were blocked in total.

Interestingly this rule was again instrumental in stopping a run of attacks which included links to web-hosted malware spoofing the US Internal Revenue Service.

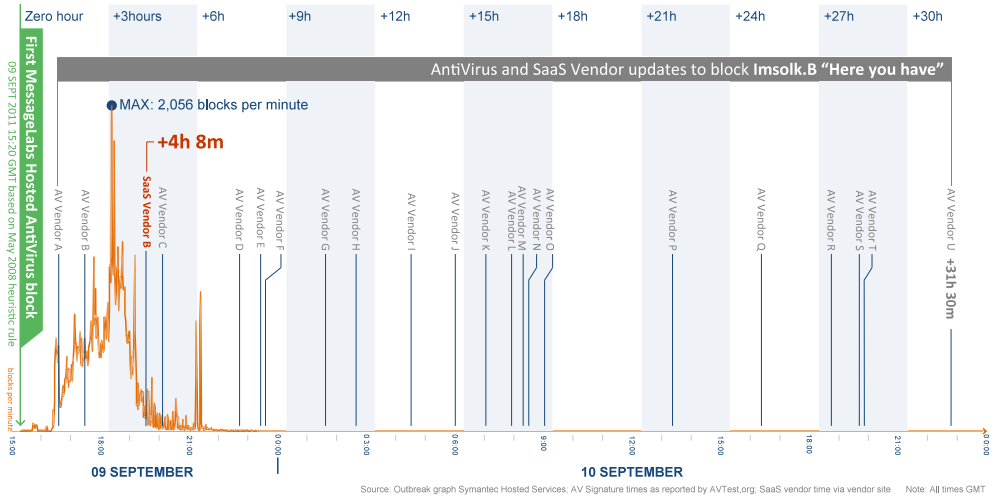


Figure 32 Imsolk.B outbreak

The attack used a technique that is not particularly new; Skeptic™ often intercepts emails sent from machines infected with mass-mailers containing copies of the virus, or hyperlinks to viruses hosted on compromised web sites. A favored social engineering technique that has been used previously is the "virtual postcard" technique: an email arrives stating the recipient has received an online e-card with instructions to click the hyperlink to view it. The link would then lead the recipient to download a viral executable that when run, immediately begins to spam itself out to any email addresses it finds on the victim's computer.

This attack used many of the same techniques but the social engineering was significantly different.

Since the emails were sent from an infected recipient, using the recipient's email account and legitimate email server, the email was much more credible when compared to the usual postcard-style attacks that spoof the sender addresses. This significantly enhanced the social engineering aspect as the email may appear to be business related, appear to come from someone else with whom the recipient has a business relationship, or even come from someone in the recipient's own organization. Furthermore, some organizations mandate the use of encryption on certain correspondence and email systems automatically encrypt these messages. In these cases the email encryption makes the messages challenging for security technology to analyze.

4.2 Targeted Attacks

4.2.1 Introduction to Targeted Attacks

Almost any organization possesses sensitive and valuable data that is an attractive target for cyber criminals. One technique is to use well researched, highly customized attacks that rely on social engineering for success – targeted attacks.

The danger of targeted attacks is the stealth deployment of malicious code that quietly performs some covert operation on the recipient's computer. Sometimes this code is attached directly to an email message, but increasingly they are frequently hidden within very legitimate looking documents and even hyperlinks. The recipient only has to open the attachment using a vulnerable application, or click on a malicious hyperlink, and their computer is compromised.

4.2.2 Socially Engineered - Dressed up for the Occasion

Using very sophisticated social engineering techniques, the targeted messages are usually business-related or tied to some newsworthy event, and may be sent from a webmail account or by using a forged *From:* address crafted to appeal to the target. The email gives the impression that the attachment contains important information, such as current affairs, meetings, legal documents, agreements or contracts.

Social engineering is very important for any targeted attack to succeed. Even the most technically sophisticated malware is doomed to failure unless the social engineering used to dress up an attack is convincing. Social networking has provided a rich resource for the cyber criminals to gather strong intelligence prior to any attack.

4.2.3 Targeted Attacks on the Rise

When targeted attacks first emerged five years ago, MessageLabs Intelligence tracked between one or two attacks per week; over the course of the following year, this number rose to between one and two per day. Subsequently, attacks have increased further from approximately 10 per day to approximately 60 per day in 2010. By the end of 2010 MessageLabs Intelligence identified approximately 77 targeted attacks blocked each day.

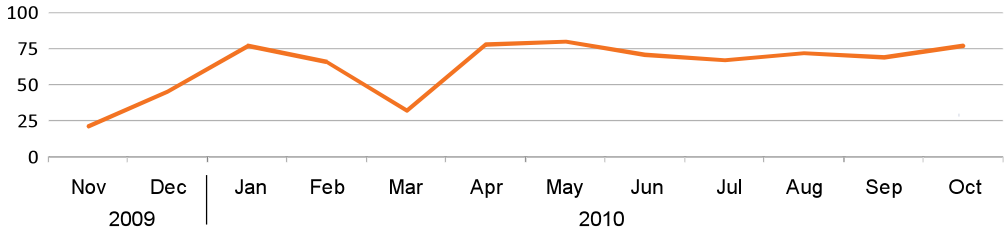


Figure 33 Targeted attacks per day

Typically, between 200 and 300 organizations are targeted each month, but the industry sector varies from month-to-month. Over time the same individuals are frequently targeted again, but each time using different exploit methods. Each exploit method may relate to a particular vulnerability within an application that has been targeted.

Targeted attacks detected by MessageLabs Intelligence can be evaluated for source and target region.[11] The greatest volume of targeted attacks detected originated in North America, followed by East Asia, Northern Europe (including the UK) and South America.

[11] NB: Since these are attacks against clients that were detected, the targeted region volume is significantly influenced by the distribution of Symantec Hosted Services clients.

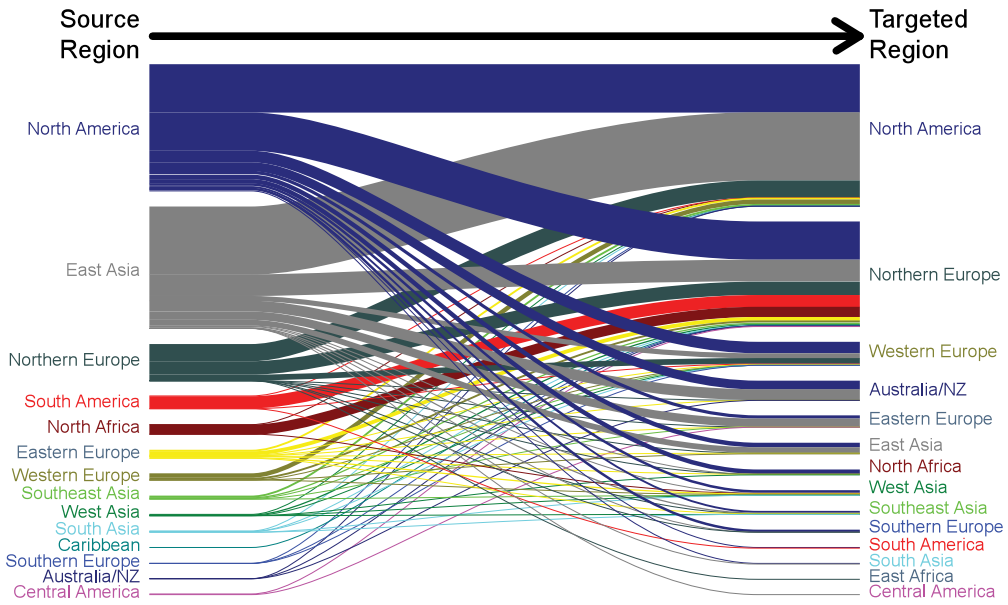


Figure 34 Targeted attack flow between regions

4.2.4 Understanding the Most Frequently Targeted Job Roles in Targeted Attacks

The recipients of targeted malware used in the commission of industrial espionage, bribery or blackmail are often of a high or medium ranking seniority within their organization.

With some simple reconnaissance, it can be surprisingly easy to collect a great deal of information about the targeted individuals; our research finds the Internet provides significant information for as many as 80% of the targeted individuals.

The top five most frequently targeted roles include:

	March 2010	November 2010
High seniority	42%	25%
Medium seniority	18%	29%
Low seniority	5%	4%
General mailboxes	19%	19%
Unknown	16%	21%

Table 6 Seniority of targeted employees

While information on mid and low seniority employees can be harder to find, attackers do appear to take the time to target these individuals. For example an attacker will sometimes target an executive assistant's or a general mailbox, perhaps in the hope that these messages would be less likely to arouse suspicion and may be more likely to be opened than an email sent to higher level employees.

Overall during 2010, there does appear to be a slight shift toward targeting lower-ranking employees.

4.2.5 More Industries are Targets

Five years ago, most targeted attacks were executed against large or well known organizations. Targeted organizations frequently included government departments, defense organizations, energy companies, pharmaceutical companies, and international trade organizations. Since then, the scope of organizations targeted

has steadily expanded and today almost any organization may be a target. While small organizations may be directly targeted it is possible the actual intent is to compromise larger organizations – attackers may be looking to partners and suppliers as the weakest link in the supply chain.

In October, MessageLabs Intelligence detected a series of attacks against companies in the retail sector. Prior to October only a few attacks were detected against retail firms but for a period of time these attacks jumped to 25% of all detected targeted attacks.

4.2.6 Compromised Web Sites and Multi-staged Targeted Attacks

There are varying degrees of sophistication for targeted attacks, and the more cutting-edge examples can be extremely difficult to recognize for anyone who is a target. An attack in June 2010, involving two defense contractors, demonstrated the degree of preparation undertaken by the attackers.

The first step in the attack was for the attacker to gain unauthorized access to the web site of Defense Contractor A and to create a fake press release directory. Into this newly created directory, the attacker uploaded a landing page, containing obfuscated JavaScript, an exploit and a malicious binary.

The second step was for the attacker to send carefully crafted emails to addressees at Defense Contractor B, the intended recipients of the malicious code. The emails purported to be from a webmail address reporting the arrest of Defense Contractor B's CEO for violating US export regulations. These emails contained a link to the malicious landing page that had been created earlier, a seemingly realistic press release directory hosted on Contractor A's genuine web site.

Figure 35 Example of the email targeted at employees of Defense Contractor B

The JavaScript on the landing page examines the web browser of the visitor and serves a different exploit to the visitor based on whether or not they are using the Firefox browser. In either case the attacker attempts to get the browser to download a second file from the same web site. This file contains two levels of obfuscated JavaScript that exploits the Microsoft Help vulnerability[12] discovered on June 9, 2010.

[12] *For more information, please visit:*
http://archives.neohapsis.com/archives/fulldisclosure/2010-06/0197.html

4.2.7 PDF Zero-day Targeted Attack Went Practically Unnoticed

In September 2010, the security industry witnessed two major threats that occurred around the same time. On September 9, as the world was learning of the IMSOLK.B ("Here You Have") outbreak, a targeted attack that had begun almost a one week earlier was almost unnoticed. On September 1, 2010 at 7:30 GMT Skeptic™ proactively identified and stopped a small number of suspicious PDF attacks containing malicious JavaScript exploiting a zero-day vulnerability in the PDF file format (CVE-2010-2883).

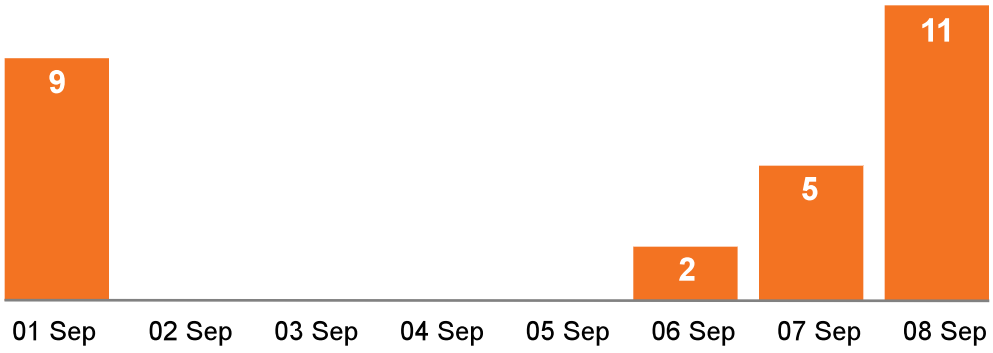


Figure 36 Zero-day PDF vulnerability (CVE-2010-2883) blocks 01-10 September

Nine copies were blocked in total on September 1, the date the attack began, and a further 11 copies at its peak on September 8; one week later when the vulnerability was first publicly disclosed.

The PDF file-type is not only just a portable document format, it has the ability to embed complex JavaScript code, which in recent years has made the PDF attachment type one of the attackers' favorite weapons. JavaScript and PDF files can be a deadly combination when it comes to targeted attack vectors.

These attacks were enhanced with the use of social engineering and used the following subjects: 'David Leadbetter's One Point Lesson', 'secret trip to China' and 'Interview Request.' They were all carrying a similar malicious JavaScript embedded in the PDF file.

4.3 The Story of Bredolab: A Brief History of Malware Evolution

Over the last three years MessageLabs Intelligence has seen the rapid growth of an interesting new approach from attackers, often referred to as "pay per install" (PPI).

The most active PPI seen is Bredolab – this malware is flexible but at its heart is designed simply to seize control of the victim's computer. Once attackers gain control, the compromised machine can be used by the Bredolab operators for their own purposes or they can rent or sell use to another attacker. These third party attackers gain access to known compromised machines and can focus on their targets rather than the challenging task of building their own stable of bots.

Once compromised the computer can be directed to download and install any variety of malware and spyware, including key-loggers, botnet Trojans, phishing Trojans such as Zeus and rogue security software.

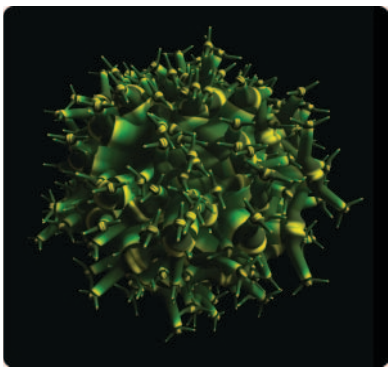
MessageLabs Intelligence has been tracking and analyzing Bredolab malware since the first emails carrying Bredolab emerged in August 2008. Over the subsequent weeks we saw the volume of malicious emails rapidly increase. In September 2008

these emails were responsible for a 17% rise in malicious email blocked by Skeptic™ – this demonstrates the considerable impact a new attack technique can have.

Bredolab malware is sophisticated, innovative and constantly evolving. Every three to four weeks since MessageLabs Intelligence first blocked Bredolab, we see one or more elements of the malware increase in sophistication, or simply change. The developers behind the malware are clearly well organized and work steadily to constantly improve the effectiveness of the malware. Some of the interesting features of Bredolab include:

- **"Anti anti-virus."** Bredolab will try to disable any existing anti-virus software on the victim's computer, and in doing so display an advanced knowledge of how many of the common endpoint anti-virus solutions work.
- **Junk code.** To obstruct analysis and interrogation by anti-virus engines, Bredolab uses junk code to make the task more complicated. The use of junk code is common but Bredolab has used it in new and innovative ways.
- **Anti-debugging technology**. Bredolab performs checks to detect if it is executing within a debugging environment, for example a malware analyst trying to step through what the malware is doing.
- **Encoded communication**. All communications between the threat and remote servers use encryption.
- **"Server-side polymorphism."** The threat constantly changes its method of packing and its appearance in order to avoid detection.
- **Self-defense.** Bredolab includes countermeasures to evade detection by traditional anti-virus technology, where a scan buffer is used to load data to be scrutinized for malicious characteristics.

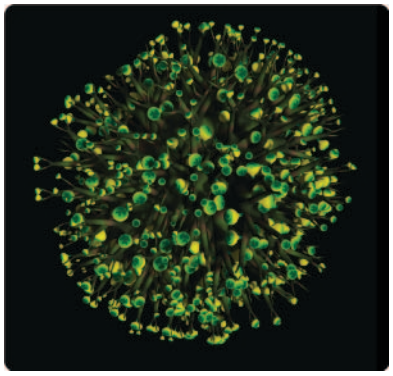
4.3.1 Timeline of Evolution

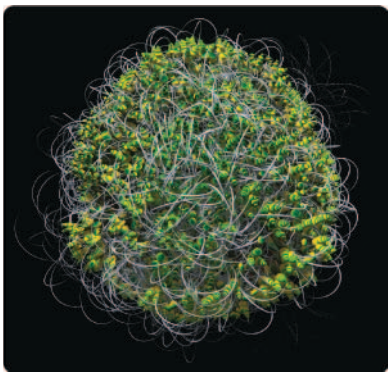


This early version of Bredolab is encrypted and packed with one of the first polymorphic codes. The first several thousand variants of this strain evaded many traditional security products before the code evolved and morphed into something even more complex.

This is Bredolab, but this version was protected with an updated polymorphic engine that was released only a few weeks after the first. The code has changed form – it tries to appear very different, but the functionality is basically the same – to act as a conduit for more malware.

Many security solutions would not recognize this as Bredolab – which is how it evades detection that may have caught earlier strains.





Another variant of Bredolab, this time it is protected by a more aggressive polymorphic packer released at the end of 2010.

It was mass-mailed with hundreds of different variants of itself, to maximize its chances for infection.

4.4 File Types in Malware

As discussed in the Spam section of the report, in 2010 it became much less common for spam to have files attached, with most spam using hyperlinks. Email size is directly related to the number of emails that can be sent. Cyber criminals face a choice of sending smaller volumes of messages with files attached or relying on other methods for delivering the malicious payload, like a piece of web-hosted malware, and sending many more messages. Because the risk of attachments is better understood, it is also much more difficult to get an attached file past filters than it is text or links.

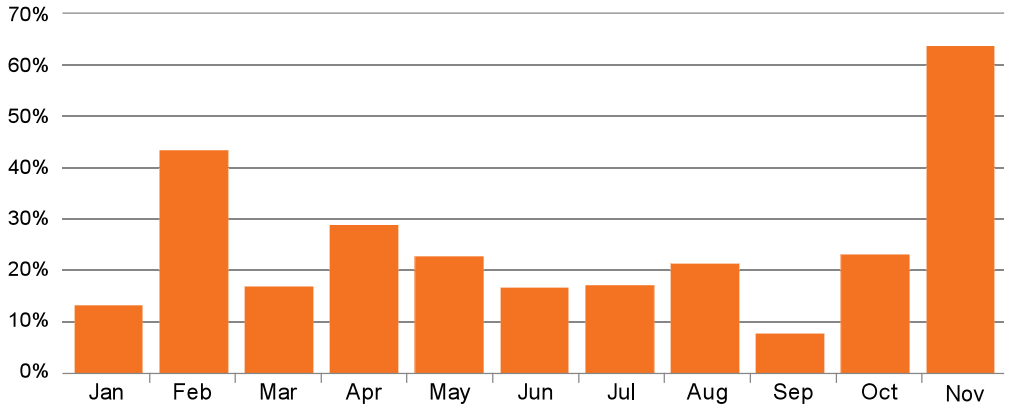


Figure 37 Percentage of malware that is a link

The Bredolab malware is an example of malware contained in compressed archive attachments. The Cutwail botnet was well known for distributing the Bredolab malware, as discussed earlier, which was often disguised as delivery notifications from well-known shipping companies.

Emails containing malware are generally bigger than typical spam, as they contain some kind of executable code, or exploitable file. Eighty-eight percent of malicious mails are over 10kB, with over 26% ranging from 90 to 100kB.

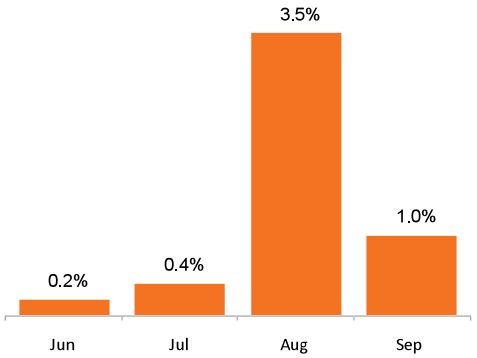


Figure 38 Percentage of spam containing a compressed archive

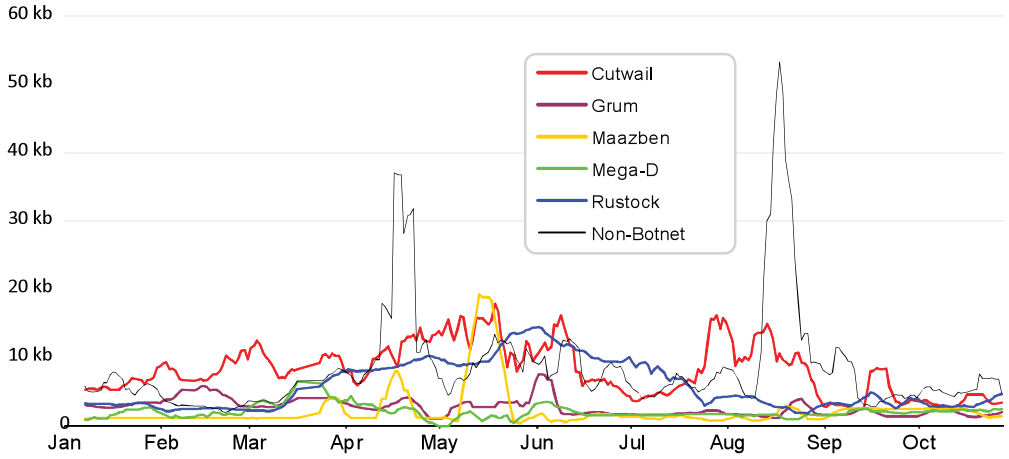


Figure 39 Average size of email containing malware

However, the average size malicious email varies much more from day to day. On any given day, it is rare for the average size of malware to fall lower than 10KB.

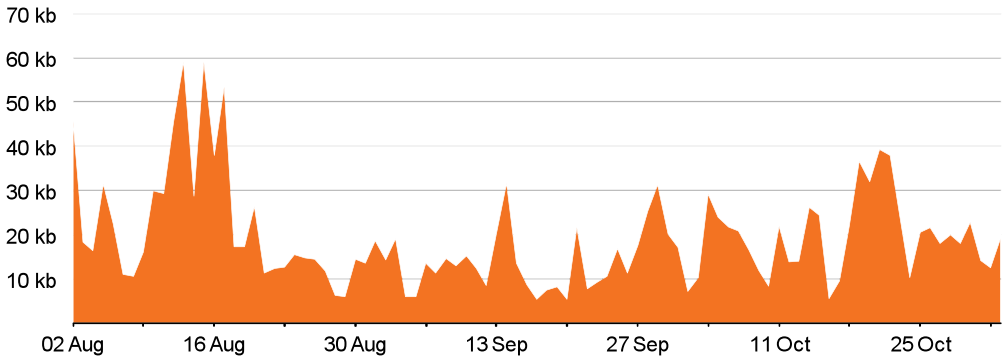


Figure 40 Average size of email

Figure 40 shows that there was a distinct rise in the daily average file size in August. This rise occurred for the same reason as the spike in spam around the same time - a large run of compressed archives from the Cutwail botnet spreading the Bredolab family of malware.

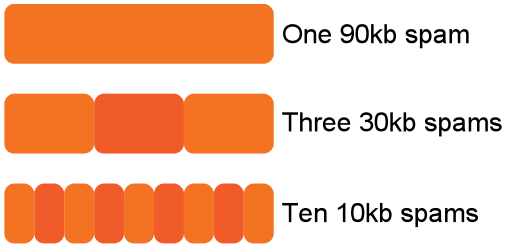


Figure 41 Spammers Dilemma: Size or volume

The size variation visible in Figure 40 occurs as malware tends to be sent in runs -- just like spam -- with each run having a different type of malware. A run with an attachment will have an impact on the average size of messages disproportionate to the volume of messages sent, since the attachments are usually far larger than typical text-based spam.

5 WEB: TOP THREATS OF 2010

5.1 Introduction to Web-based Risks

Globally, almost 2 billion people use the internet[13]. Everyday hundreds of millions of visits are made to web sites worldwide. But as usage continues to climb upward, some accepted truths about the web have broken down. A few years ago, common sense was all that was needed to keep a computer free from infection by avoiding the malware that lurked in the shadier corners of the internet. But today, that has changed.

In 2010, the average number of web sites blocked as malicious each day rose to 3,066, compared with 2,465 in 2009; an increase of 24.3%. In 2010, MessageLabs Intelligence identified malicious web threats on 42,926 distinct domains, the majority of which were compromised, legitimate domains.

In 2010, the threat posed by the web is more acute and extensive than before. Almost any web site can now be used to host malware or redirect visitors to one that does. Indeed, an infection is much more likely to result from a visit to a perfectly legitimate web site that has been compromised with a virus or spyware than from one set up specifically to spread malware. In addition, techniques such as drive-by downloads have become commonplace, where simply visiting an infected site is enough to infect a computer.

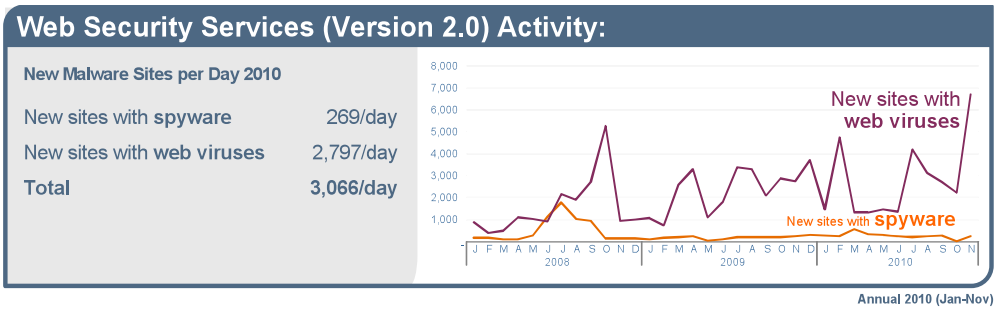


Figure 42 Web Security Services activity

Once malware has breached business defenses, sensitive systems and confidential data may be exposed to damage or theft, potentially resulting in loss of revenue, loss of intellectual property, loss of proprietary data, damage to reputation and exposure to legal action. For the increasingly skilled cyber criminals behind such attacks, their intent is clear: to seize control of victims' computers and then use that control in a variety of crooked ways.

[13] http://www.internetworldstats.com/stats.htm

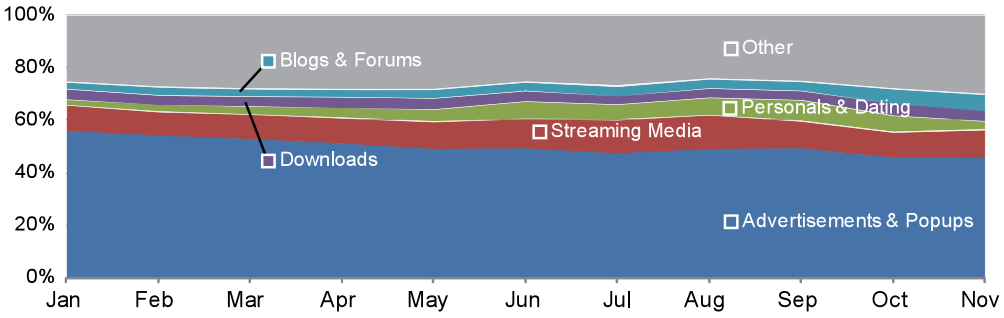


Figure 43 Web policy blocks

5.2 File Types in Web Hosted Malware

MessageLabs Intelligence detects a wide range of malicious file types when blocking web malware.

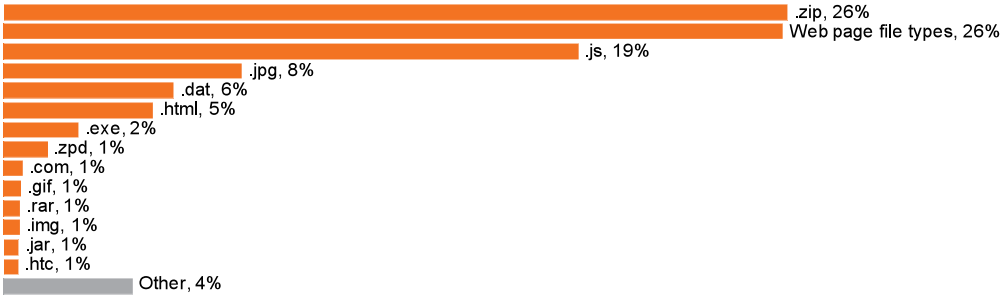


Figure 44 File types in web malware

.Zip files were the most commonly blocked in 2010 driven by a few outbreaks.

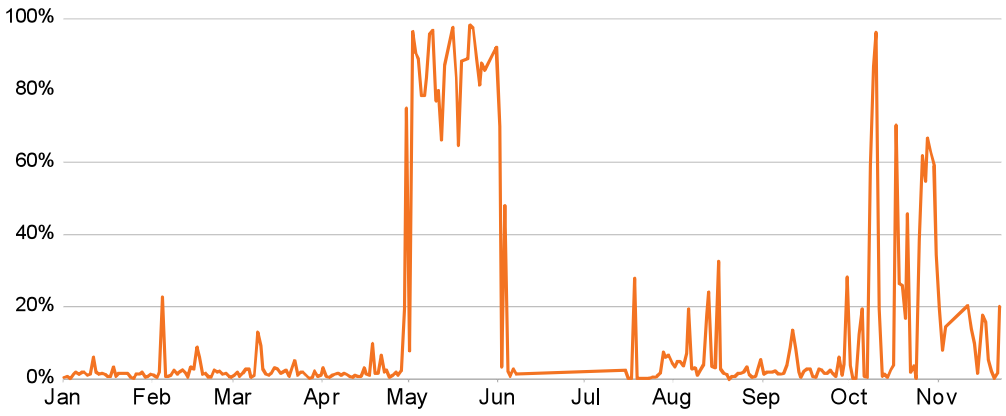


Figure 45 Percentage of .zip files detected in web malware

Almost all the .zip blocks in May were the same file on a web site created to purposely house malware for download. The web site was hosted on a Portuguese hosting company, and has been shut down for violating terms of service (by hosting malware).

5.3 Employee Browsing Habits: The Good, the Bad and the Ugly

In September 2010, MessageLabs Intelligence examined the importance of IT and HR managers understanding that there will always be a subset of employees likely

to try and flout the rules when browsing the internet. This behavior not only goes against company policy, but also wastes time and can be a serious drain on resources and bandwidth, increasing the risk of infection by malware.

When considering the risk profile of an organization, users may be grouped together according to their behavior patterns and a “bell-curve” of normal distribution ensues. At one end of the curve will be the employees who, by their compliance with policy and online habits, present a minimal risk to the organization. In the middle will be the majority, who present a tolerable organizational risk. At the extreme end is the small number of users who present the greatest level of risk.

For all employees browsing the web, approximately one in five (18%) requests are blocked but web browsing behavior differs from employee to employee. It is important to understand which employees present the greatest level of risk to an organization.

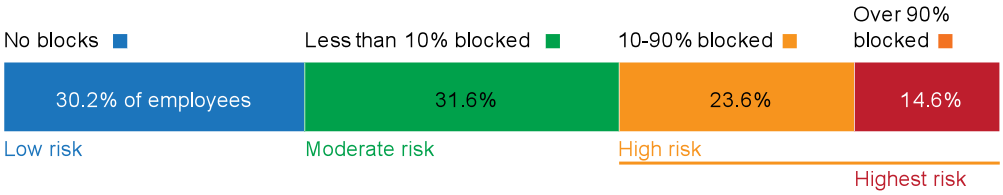


Figure 46 Blocked web requests by percentage of employees

Figure 46 shows that employees browsing the web fall into three distinct groups:

- ***Low-risk Users*** - Approximately one-third of users don't have any blocks among their requests, in other words all sites requested are within company policy and not malicious (blue in Figure 46)
- ***Moderate-risk Users***- Approximately one-third of users account for fewer than 10% of all requests blocked (green)
- ***High-risk Users*** - The remaining third of users have a higher proportion of requests blocked, accounting for over 80% of the blocks. The highest risk 14% of users on their own account for 20% of blocked requests (marked red)

This latter group represents behavior that is firmly against company policy, but rather than the expected bell curve, employees are either very well behaved or very poorly behaved, from the point of view of their employer.

A request can be blocked either because accessing the web site is against company policy or because the site contains malicious content. In many ways it is not just about the number of requests blocked, but also about the users’ intentions. For example, accessing social networking web sites, webmail accounts and some news web sites may be against corporate rules, but most employers are unlikely to consider it a serious threat, unless it caused drain on bandwidth or wasted productivity. But visits to web sites containing tasteless or offensive material and adult sexually explicit material, would surely give an employer cause for concern.

By comparing the second category of users in Figure 46 (green) with the third category of users (orange and red), it is possible to build a profile of the types of users involved. Overall, the average number of blocks per user is eight times higher for the high-risk users, than for the moderate-risk users. Not only do high-risk users have a higher proportion of requests blocked, but the number of requests blocked was generally much higher overall.

The high-risk users seem to generate more requests for web sites that conflict with company policy, and blocks triggered for the “Proxies & Translators” category were

five times higher for this group of users – highlighting a clear attempt to circumvent company policy to gain access to blocked web sites.

Moreover, “Advertisements & Popups” were 2.6 times more likely to be blocked for high-risk users – this suggests that even when they visit web sites that are not directly blocked, these sites attract much higher advertising and pop-up traffic. It is very common for malicious attacks to take place via advertisements or “malvertisements” that are served up on otherwise harmless sites. The advertising provider may have been compromised and used to serve malicious JavaScript for example. This means that this category of users is more likely to encounter advertisements and malvertisements, potentially leading to malware infections.

For all users approximately one in 2,000 (0.05%) web requests were blocked as malicious, equivalent to one malicious web site blocked per user every 10 days. Moreover, the proportion of requests blocked as malicious for high-risk users was 7.6 times higher than for moderate-risk users.

Finally, requests from high-risk users triggered blocks for twice as many unique domains; with 1.4 domains blocked per user per week, compared with moderate-risk users who had 0.7 domains blocked per user per week.

Not only did high-risk users trigger more blocked web traffic and a higher proportion of blocked web requests, but they also had blocks against a wider variety of web sites, highlighting the additional level of risk to the organization in terms of malicious infections.

5.4 Web-based Risks from a Mobile Workforce

One of the greatest challenges for IT managers in recent years has been how to secure an increasingly mobile workforce. With many businesses finding themselves in a fiercely competitive market as many economies recover, more workers are spending longer hours on the road or working from home.

Recently MessageLabs Intelligence featured analysis of roaming users’ web browsing habits extending the research described in the previous section. This work highlighted that employees who work both in and out of the office showed higher-risk behavior profiles when roaming than when in the office; 35% of users that were both office-based and mobile had a higher proportion of web requests blocked when roaming, compared to when in the office. Moreover, users who were always mobile actually exhibited relatively good behavior patterns.

Based on their mobility, MessageLabs Intelligence examined more closely the three categories of users and their web behavior profiles:

- ***Office-based*** – Users for whom all web browsing activity is confined to the physical corporate network. These users are never mobile or work from home.
- ***Nomadic*** – Users that are always on-the-road, working from home or from other networks.
- ***Mixed-location –*** Users that are sometimes in the office and sometimes off-site or working from home.

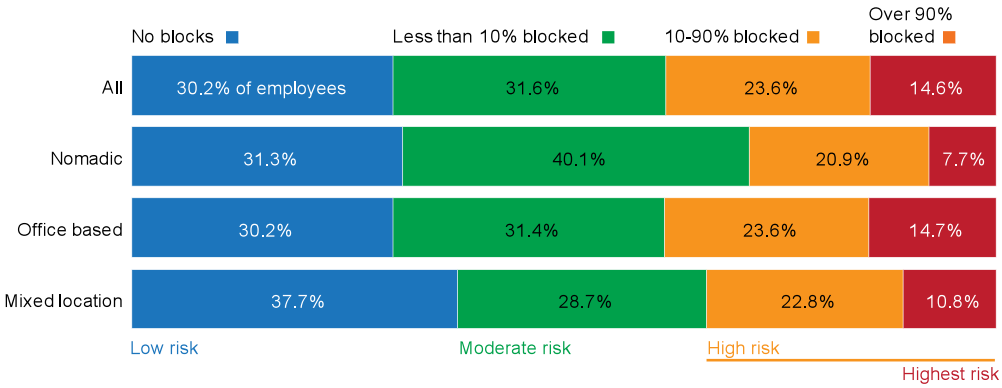


Figure 47 Blocked web requests by percentage of employees

Figure 47, illustrates that nomadic users actually experience a slightly lower proportion of blocked requests with their behavior being slightly less risky than the average for all users. Users that were both mobile and office-bound exhibited behavior that was better than the overall average, but slightly worse than for nomadic users.

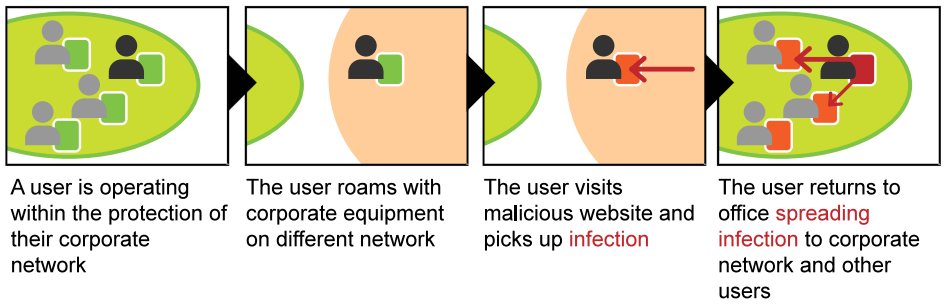


Figure 48 Bringing malware back into the corporate network

It seems that nomadic users behave in a similar manner to office-based users, whereas those that have mixed locations follow policy while in the office, but when off-site, they appear to relax their browsing habits considerably. This lax behavior is not only contrary to company policy, but increases the risk of infection from malware.

Top 10 Web Blocks: Office Based	%
Advertisements & Popups	48.7%
Streaming Media	10.5%
Personals & Dating	7.7%
Downloads	4.0%
Blogs & Forums	4.0%
Games	3.1%
Chat	2.5%
Adult/Sexually Explicit	2.5%
Computing & Internet	2.1%
Search Engines	0.8%
Shopping	0.6%

Top 10 Web Blocks: Roaming	%
Streaming Media	22.8%
Downloads	21.5%
Advertisements & Popups	19.7%
Personals & Dating	10.9%
Shopping	3.6%
Search Engines	2.9%
Chat	2.5%
Computing & Internet	2.4%
Games	2.4%
Blogs & Forums	2.1%
Adult/Sexually Explicit	1.9%

Figure 49 Web blocks: office-based versus roaming

Figure 49 shows examples of browsing behavior worsening as users leave the corporate network, but continue to use corporate equipment. These are examples

of users that fall into the category of high-risk and represent the actions of 35% of mixed-location users cited earlier. These users are likely to attract the attention of the HR department.

Technology plays a fundamental role in reducing risk from employee browsing behavior, but equally important is user education. It is important that staff understand the importance of the organization's security policies; individual employees need to understand that they also have a role to play in their company's security. It is a three-pronged approach - leave any one of these elements out then the business may be vulnerable to exposure.

5.5 Trends in Web-based Policy Controls

Balancing control and access is an ongoing challenge for IT decision makers. The question becomes not whether employees' online behavior should be managed but rather what extent of management is sensible and acceptable. What may be appropriate for some organizations may not be suitable in others. Some companies may choose to take a more relaxed approach while others may wish to lock everything down. Some employees may require full access to the Internet with some departments or individuals given more latitude than others.

Recognizing this need for more flexible web access, businesses in 2010 are tending toward a more granular approach to control, with an increased use of permitted "allow-lists" replacing the blanket "block-list" approach in previous years.

Understanding how web policies work.

There are three elements that make up the policy based control in the MessageLabs Hosted Web Security Service

Rules: Rules tell the service to evaluate each web request to see if it meets particular criteria. These criteria can include specific URLs (e.g. Symantec.com), categories of URLs (e.g. Advertising & Pop-ups), a time period, a particular employee or group of employees (e.g. all sales employees).

Policies: Rules are grouped into policies.

Actions: Actions are applied against policies. There are four actions:

- Allow
- Allow and log
- Block
- Block and log

Rules tell the system what to look for when requests are made, allowing modification for who is asking and when the request is made. Policies that group these rules and actions tell the system what to do with the request. Depending on how the policies are ordered this approach allows for very granular control over an organization's web traffic and usage.

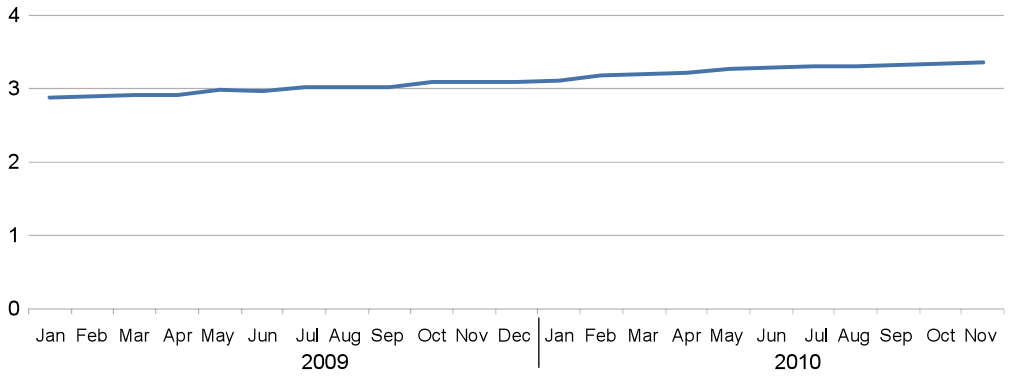


Figure 50 Allow policies per organization

Starting with a default rule of "no access allowed," it is more common for businesses to create highly customized policies that relax web site access controls for pre-approved web sites. Figure 50 highlights the growth in the number of policies used to restrict access to certain sites – particularly for streaming media, web-based email, games and shopping web sites – but allow policies have grown at a higher rate.

For example, a single policy may include a large number of URL-based rules, grouping together generally allowed web sites, while another policy will include additional rules covering lunchtime-only access for certain web sites or limiting access to certain groups of people.

The number of allow policies has grown at an average rate of 0.8% per month in 2010, compared with 0.6% per month in 2009.

The average number of policies for each organization has increased from three in 2009 to 3.3 in 2010; each policy containing a large number of custom URL-based filtering rules. The most common allow policy implemented in 2010 was to grant access to Twitter.

The average number of block policies increased during the first half of 2010, but subsequently leveled-out. In 2010, the average number of block policies per organization was 2.4, compared with 2.3 in 2009.

This suggests that organizations are choosing to block more rigidly with their default policies and to use more whitelists to provide more granular access to particular web sites for specific departments, individuals and time periods. As with the allow policies, block policies also contain many custom URL rules. The most common block policy created in 2010 was related to controlling access to the YouTube web site.

Furthermore, the number of custom rules per organization has been increasing steadily each month. These rules are then applied in both allow and block policies.

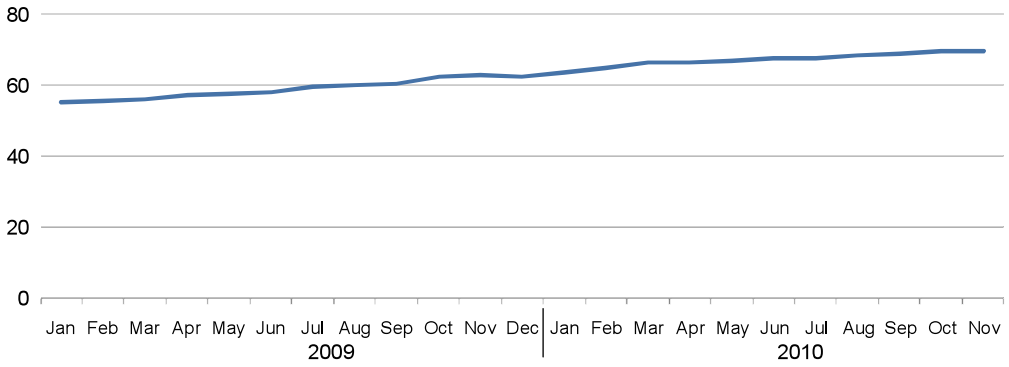


Figure 51 Average number of custom rules per organization

In 2010, each organization had an average of approximately 70 custom rules, compared with 60 in 2009. MessageLabs Intelligence expects this number to surpass 100 by the end of 2011, as businesses become more aware of the risks associated with unrestricted web access.

Rules related to Facebook, MySpace, Twitter and YouTube were the most common custom rules in 2009 and remain so in 2010. This year also saw the emergence of rules relating to LinkedIn, which had appeared in few custom rules.

5.6 Legitimate Web Sites Exploited in Web Attacks

5.6.1 Malicious Web Sites

Safeguarding against malicious web sites is not a matter of policy as they often do not fall under any particular category, such as Adult/Sexually Explicit material. In theory almost any web site is capable of hosting malware or forwarding to a web site that does. Web sites can be set up and hosted by criminals, or legitimate web sites can be compromised. One malicious web site, visited by one unsuspecting user may be all that is required to breach the defenses of a business, and cause disruption, loss or damage to reputation. For example, sensitive systems could be accessed, malware could spread within the company networks, or valuable information could be stolen.

Malicious web traffic can be classified as either spyware or malware. Of all malicious blocks in 2010, the split is approximately 4% spyware, 96% malware. URLs that are blocked as spyware may include pop-up ads, attempts to track browsing behavior or attempts to change the way a browser operates. URLs can be blocked as malware for many different reasons, but there is no grey area with malware – it is almost certainly trying to do something bad. The ultimate danger is always the same: either to get some malware onto the target computer or to gain access to personal details or confidential data.

In 2010, the number of malicious web sites blocked per client each month was 20.2% higher than in 2009. March 2010 saw the highest average number of malicious web blocks, per client, per day since 2009; an average of 1.4 malicious blocks per customer per day. In 2010, users in EMEA were most likely to encounter malicious web sites. In 2009, users in APJ were likely to encounter malicious sites.

The malicious domains serving malware change faster than the malware itself. Attackers still work hard to continuously create new malicious web sites, or compromise legitimate domains to serve malware. One threat is often repeatedly used on multiple malicious web sites. In 2010, almost 90% of malicious web sites blocked were for legitimate, compromised web sites, compared with 80% in 2009.

On average malicious web threats survived longer in 2010, making it more likely that web users would encounter dangerous web sites.

For the cyber criminals, it can be costly to produce new families of malware to maintain their criminal activity at sufficient levels. Registering new domains is much more economical for them, and by spreading the malware across as many different web sites and domains as possible, the longevity of each new malware is increased. When deploying server-side polymorphism, operating a web server that hosts malware files and running software that generates new malware variants each with its own unique signature every few minutes or hours, the same family of malware code may be packaged differently into new strains, automatically and dynamically, each time it is accessed. This requires a different anti-virus signature each time in order to detect it accurately. These approaches combined with the use of "bullet-proof" hosting services, service providers that are difficult to shut down, and "fast-flux" hosting, a technique used by some botnets to hide phishing and malicious web sites behind an ever-changing network of compromised hosts acting as proxies, means that criminals can ensure that malicious web sites are not taken down quickly in response to complaints.

In many cases the organized criminals often have highly automated techniques in place that require little or no monitoring, and their systems are automatically working day and night compromising as many legitimate web sites as possible and registering new ones. Once these processes are in place, a compromised web site can be re-configured remotely depending on what method the attackers are using.

5.6.2 Decline of Web Sites Registered for Malicious Intent as Cyber Criminals Compromise Legitimate Sites

When looking at the domains behind malicious URLs, it's interesting to consider if the domain is legitimate or newly set up with malicious intent. An effective way to do this is to look at the date that the domain was registered.

Generally if a domain is registered less than three months before MessageLabs Intelligence first blocked the URL, it is very likely that the domain was registered with malicious intent. If the domain was registered greater than three months before MessageLabs Intelligence first blocked the URL, the domain is likely to be a legitimate compromised domain.

	2009	2010
Young domains	20.2%	12.5%
Old domains	79.8%	87.5%

Table 7 Percentage of old versus young domains

In 2010, almost 90% of malicious web sites blocked are legitimate, compromised web sites. Many web users believe (as was once the case) that the most dangerous web sites to visit are those with adult or sexually explicit content, but this is no longer the case. Users browsing the web are actually more likely to stumble on malware when they are going about their normal, everyday, surfing habits.

Attackers have realized that it is better to lead victims to malware via legitimate web sites, than to try to lead users to purely malicious domains. There could be many explanations for this, but three possible reasons are:

- Visitors to legitimate web sites will be less suspicious and/or less suspecting of malware

- If attackers compromise web sites with a high volume of visitors, the potential to infect users is much higher than if they tried to lead people to newly set up domains
- The lifetime of the threat is prolonged when compromising legitimate web sites versus serving up malware on new domains, which can be taken down quickly and easily.

5.6.3 Lifetime of Malicious Domains - How Long Does a Malicious URL Remain a Threat?

The owners of legitimate, compromised domains will almost certainly be unaware for days, perhaps weeks, that their web site contains (or redirects to) malicious content.

Once a domain is used to serve malware to unsuspecting visitors, it is usually not long before the domain is recognized by the security community and may appear in a block list. Once blocked, steps are then taken to issue a notice and takedown to the registrar or hosting provider to remove it as a threat from the Internet. However, in the case of compromised, legitimate web sites, the owners should be notified that their web sites have been compromised and given the opportunity to take appropriate action to clean up their sites, removing the malware and closing any vulnerability that was exploited to gain access.

How long, on average, does it take for a malicious web site to be noticed and then removed or rendered harmless again?

The research indicates legitimate domains, when used to host malicious content, actually survive for a longer period of time than their younger counterparts and take a relatively long time to be cleaned. Only 2.3% of legitimate or older web sites are cleaned up within one day; 3.7% within two days; and 6.9% within one week.

Why does it take longer to clean up legitimate web sites? There may be a couple of explanations:

- Taking down a “new” malicious domain is relatively easy. Finding the malicious parts of a sometimes large and complex, legitimate and often “older” web site, and then repairing it without causing damage to the operation of the web site, is much more difficult
- Once the compromise has been identified, steps are needed to secure the web site against further attack. Most companies, especially large ones, may have to go through several stages internally to achieve this. In some cases, the threat may be so deeply knotted within the structure of the web site that it may take web site administrators a much longer time to identify a mitigation strategy and implement it

It is now taking longer to deal with malicious sites, old and new, than it did in 2009:

	Young domains		Old domains	
	2009	2010	2009	2010
Threat removed within 7 days	25.4%	22.0%	8.8%	6.9%

Table 8 Domains removed within seven days

Why are threats taking longer to be removed or cleaned up? Attackers are using methods that are harder to remove from compromised web sites:

- In the case of “old” domains, attackers may be changing the content of web sites in ways that are harder to recognize

- In the case of young or newly registered domains - attackers could be increasingly registering new domains with selected registrars, particularly where it is harder to have the domain taken down
- In the case of attackers using “malvertisements” on legitimate, compromised web sites, perhaps they increasingly target advertising companies known to be poor at policing the submission of potentially malicious ads, or are easily compromised
- Legitimate web sites are becoming more and more complex, and the administration behind the web sites is more complicated, making it increasingly difficult to unpick any changes made by attackers and to resolve issues that may lead users to become infected

The bottom line is that web-based threats remain active for much longer in 2010, making it more likely that web users will encounter dangerous web sites.

6 PHISHING, FRAUD AND SCAMS: TOP THREATS OF 2010

6.1 Phishing Summary

In 2010, the average ratio of email traffic blocked as phishing attacks was 1 in 444.5 (0.23%), compared with 1 in 325.2 (0.31%) in 2009. More than 188.6 million phishing emails were blocked by Skeptic™ in 2010. Approximately 95.1 billion phishing emails were projected to be in circulation during 2010.

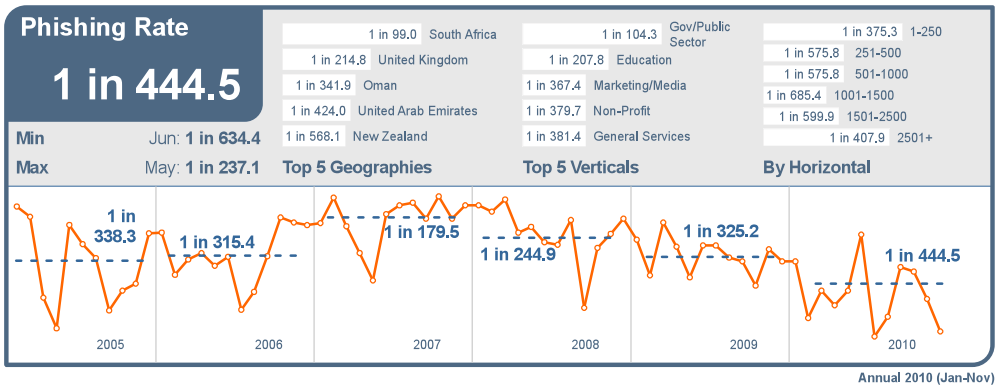


Figure 52 Phishing rate

In 2010, MessageLabs Intelligence tracked phishing attacks impersonating or relating to 1,530 different organizations, compared with 1,079 in 2009.

In 2010, impersonations of five organizations made up 50% of all phishing attacks, as compared with eight in 2009. The most frequently spoofed phishing organization was a well known international bank, accounting for 14.9% of phishing attacks blocked in 2010. The second most frequently blocked phishing attack impersonated an online retailer.

Spear phishing

Spear phishing against businesses, where the sender address was forged to appear as though it was sent from an internal employee, accounted for 6.3% of all phishing emails blocked in 2010.

6.2 Scams Adapting to News and Current Events

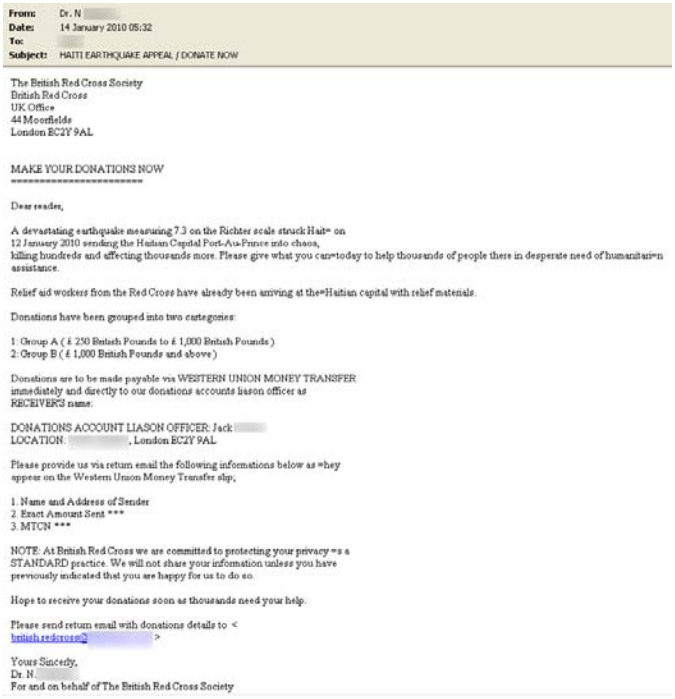
As discussed in the spam section of this report, spammers and scammers produce spam campaigns relating to most major newsworthy events.

These news-based approaches are often combined with “419” scams. The basic premise of a 419 scam (also commonly referred to as an advance fee fraud scam) is that the recipient is entitled to, or can take advantage of, some benefit and merely has to provide information or banking details to receive the benefit.

6.2.1 Haiti Earthquake Scams

Following the major earthquake that caused a humanitarian disaster in Haiti on January 25 2010, people the world over were feeling a great deal of sympathy for the country’s population. Aid was quickly offered by many countries and many charities sought donations to provide support.

However, there were also cyber criminals who took the opportunity to exploit the general public's good nature, concern and desire to help by spamming out fraudulent advance-fee fraud "419" scam emails hoping that the desire to help may cloud a person's better judgment preventing recognition of the scam for what it is. Something like the humanitarian crisis of the Haiti earthquake was, sadly, a prime target for these scammers.



From: Dr. N
Date: 14 January 2010 05:32
To:
Subject: HAITI EARTHQUAKE APPEAL / DONATE NOW

The British Red Cross Society
British Red Cross
UK Office
44 Moorfields
London EC2Y 9AL

MAKE YOUR DONATIONS NOW

Dear reader,

A devastating earthquake measuring 7.3 on the Richter scale struck Haiti on 12 January 2010 sending the Haitian Capital Port-Au-Prince into chaos, killing hundreds and affecting thousands more. Please give what you can today to help thousands of people there in desperate need of humanitarian assistance.

Relief aid workers from the Red Cross have already been arriving at the Haitian capital with relief materials.

Donations have been grouped into two categories:

1: Group A (£ 250 British Pounds to £ 1,000 British Pounds)
2: Group B (£ 1,000 British Pounds and above)

Donations are to be made payable via WESTERN UNION MONEY TRANSFER immediately and directly to our donations accounts liason officer as RECEIVER'S name:

DONATIONS ACCOUNT LIASON OFFICER: Jack
LOCATION: , London EC2Y 9AL

Please provide us via return email the following informations below as they appear on the Western Union Money Transfer slip,

1. Name and Address of Sender
2. Exact Amount Sent ***
3. MTCN ***

NOTE: At British Red Cross we are committed to protecting your privacy as a STANDARD practice. We will not share your information unless you have previously indicated that you are happy for us to do so.

Hope to receive your donations soon as thousands need your help.

Please send return email with donations details to <
british.redcross2 >

Yours Sincerely,
Dr. N
For and on behalf of The British Red Cross Society

Figure 53 Haiti earthquake scam spam

Figure 53 is an example of an email that MessageLabs Intelligence identified as a scam. The fraudsters used the correct postal address for the charity being spoofed, but the charity does not use this payment processor for donations. Also, the email address supplied for contact was not connected with the charity being exploited. Any money sent using the instructions in this email would certainly not be used to help anyone in Haiti; it would likely end up in the pockets of the cyber criminals.

6.2.2 2010 FIFA World Cup

The 2010 FIFA World Cup was exploited by a wide variety of scammers. The most common World Cup scam is the simple (and classic) lottery scam, which informs the recipient that they have won a sum of money in a lottery. These scams have been around for years and the concept is simple, but the precise details of the scams are always changing.

6.2.3 Tax Rebate Scams in the UK

In 2010, the UK's tax collecting agency, HMRC, announced that six million people in the country had paid the wrong amount of tax and stated that it would start sending letters to the affected people. Depending on their circumstances, people would be invited to claim overpaid tax back, or send a demand for payment of unpaid tax.

It was not long before MessageLabs Intelligence identified phishing emails dispatched to take advantage of the confusion caused by the announcement. In 2010, phishing attacks spoofing messages from HMRC accounted for 10.8% of all phishing emails blocked globally, compared with 0.7% for the US Internal Revenue Service.

6.2.3.1 *"Picture-in Picture" Scam*

One particularly interesting phishing scam blocked during September 2010 was notable because of the novel "picture-in-picture" technique used to disguise the message as a PDF file.

Although it does not directly refer to the HMRC announcement about incorrect tax payments, it was still likely to trick people into revealing confidential information about them in the hope of receiving a windfall.

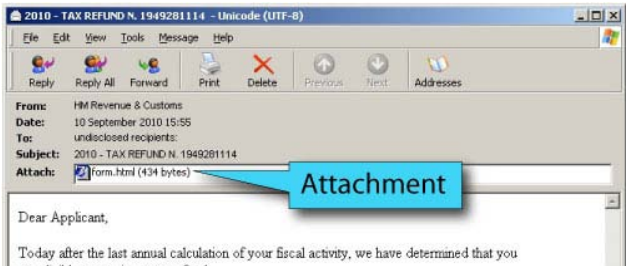


Figure 54 Picture-in-picture scam email

As seen here, the phishing message claims that the recipient is entitled to a refund, and includes an HTML attachment, which when opened uses HTML frames to load the fake web site (since taken offline), which was hosted on a compromised web server.

The web site was noteworthy as it used a "picture-in-picture" attack to disguise the page to appear as though it were a PDF document being displayed within a web browser using a plug-in. A picture-in-picture attack involves a combination of images and screenshots used to mimic the on-screen controls and appearance of an application (such as a PDF reader) or, in some cases, a whole Windows desktop. This phishing web site includes a background image, shown in Figure 55, which is a modified screenshot of a popular PDF viewer application

The text and form-fields are then overlaid on top of this background, making it look like a genuine PDF (as seen here). This technique may provide a sense of legitimacy.

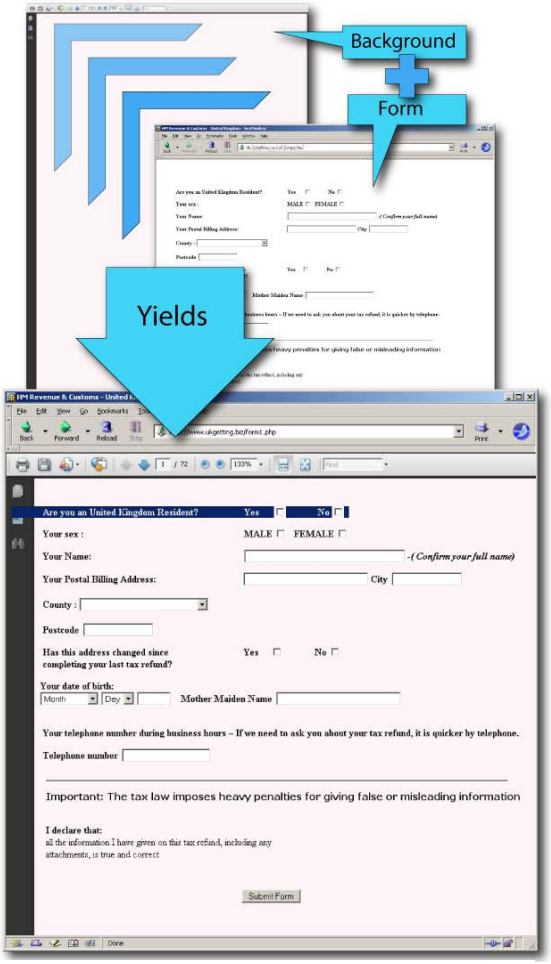


Figure 55 How the picture-in-picture HTML is constructed to look like a PDF

7 CONVERGED THREATS: A FOCUS ON SOCIAL MEDIA

This report has highlighted a wide variety of spam, malware, phishing and web tactics used by cyber criminals. As real world examples of each attack are examined it is often the case that the attackers use a sophisticated blend of tactics, spanning protocols, to maximize the potential for success. We call these converged threats.

As social media and Web 2.0 applications have grown in participant numbers and capability over the last few years, public and private social media tools have become increasingly relevant to businesses. Likewise, cyber criminals have recognized opportunities to conduct their criminal activity in new and innovative ways. The intersection of these new social technologies and more traditional modes of attack provide an excellent lens through which to view converged threats.

In 2010, many social networking platforms and social media web sites have been routinely abused and exploited. These services provide a rich seam from which personal information can be tapped about an individual in reconnaissance as a prelude to a more targeted attack. Social networking web sites are being phished to gain access to real accounts and there have been examples where rogue third-party "apps" have been created that may subsequently be added to users' profile pages. Even legitimate apps may be vulnerable to being exploited where vulnerabilities may exist in the web site in just the same way as many other legitimate web sites have also been compromised and used to host malware.

The convergence of threats across multiple protocols makes it much harder to secure online applications, especially against attacks using sophisticated social engineering techniques. For example, an email spoofing a popular social networking site may contain links to a web site harboring malware. These same links may also be shared across IM (Instant Messaging), or posted on comments pages of legitimate blog web sites.

As the threats converge, so do the ways in which we access this information; users are increasingly accessing business data while on the move, from home, or indeed anywhere other than from within the controlled confines of their corporate network. Mobile devices and smart phones are used to read and send email, to access the web and to tunnel into company networks.

In early 2011 the MessageLabs Intelligence Blog will focus on a number of these converged attacks involving social media, the risks presented by social media and potential solutions. Visit the blog[14] and subscribe.

[14] http://www.symantec.com/connect/symantec-blogs/messagelabs-intelligence

8 GLOBAL AND BUSINESS: TOP THREATS OF 2010

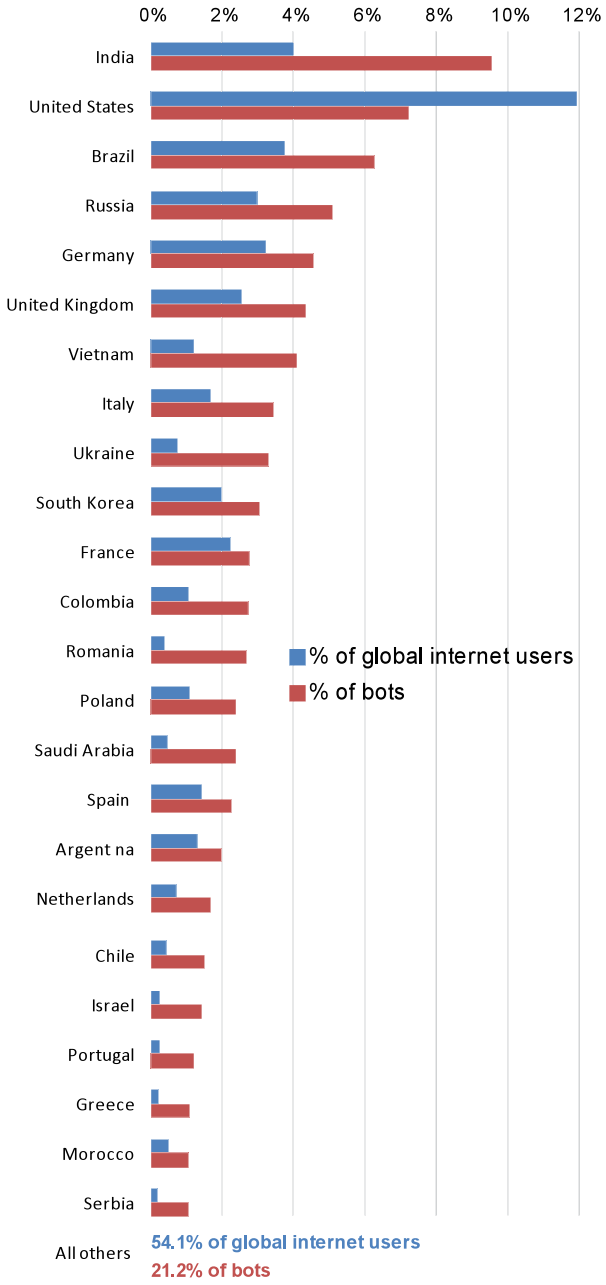
8.1 Exposure to Cyber Threats and Botnets

In 2010, 50% of global bot infections were found in just 10 countries, compared with 2009 when 66% of bots were located in 31 countries.

8.1.1 Countries Sending the Most Spam

China and India have the largest populations, far higher than any other country.

- China with 19% of the global population has an internet penetration of 32% and is home to 21% of global internet users. Despite this, China only sends 0.33% of global botnet spam. Bots do not have a strong foothold in China, despite the enormous number of internet users active there.
- China still sends an estimated one billion spam emails every day and has an estimated 17,000 active bots. In China, internet users are least likely to be part of a botnet, where approximately one in 23,700 broadband users is part of a botnet. China was listed forty-ninth in the list of countries sending botnet spam. On average, two botnet spam emails were sent per broadband user each day.
- Nigeria has a similar likelihood to China that internet users will be part of a botnet: one in 24,000 broadband users is part of a botnet. However, the profile in Nigeria in terms of population and internet users is quite different; Nigeria accounts for 2% of the global population, but has a similar level of internet penetration to China, with 29%. Like China, the proportion of botnet spam originating from Nigeria was just 0.03%.



- India is home to 17% of the world's population, but had a relatively low internet penetration rate of just 7%. However, owing to its large population number, 4% of global internet users were located in India. From this 4% of global internet users, India is the source of 8.5% of global botnet spam, second only to the US in the list of spam sources. Punching considerably above its weight in terms of spam output, it is estimated that there are approximately 487,000 bots active in India, with one in 250 broadband users being part of a botnet. On average, 320 botnet spam emails were sent per broadband user each day
- The United States was the source of the most botnet spam in 2010. The US was home to 4.5% of the global population, and 12% of global broadband users, as a result of a broadband penetration level of 77%. The US was the source of 8.7% of global botnet spam, less than may be expected considering the larger number of broadband users found there. An estimated 368,000 bots were active in the US, with one in 653 broadband users as part of a botnet. On average, 110 botnet spam emails were sent per broadband user each day.
- Brazil is also a major source of botnet spam. Brazil is home to 2.9% of the global population and 3.8% of global broadband users, sending 5.6% of global botnet spam. There were an estimated 318,000 active bots in Brazil in 2010, with one in 239 broadband users being part of a botnet. An average of 223 botnet spam emails was sent from each broadband user daily.

Generally, there are fewer active bots in 2010 compared to 2009 and at the same time penetration of internet and broadband internet use has increased so the likelihood that users may be part of a botnet has declined globally in all but a few countries.

9 2011 TREND FORECAST

Global Spam Trends

In 2011, spam will become more culturally and linguistically diverse. The use of English in spam will fall from approximately 95% of all spam to below 90% driven by economic growth and broadband adoption in emerging economies. For instance, spammers will target Brazil with more than 40 percent of spam in Portuguese.

Portuguese and Spanish will become some of the most popular languages used in spam other than English. We expect Italy to receive 20-25% of spam in Italian, France to receive 15-20% French language spam and Germany will find 10-15% of its spam in German. China will receive 10-15% of spam in Chinese and spam in Japan will be 10-15% in Japanese. Arabic language spam will increase in the Middle East, for example Saudi Arabia will receive 10% of its spam in Arabic.

Likewise, as the internet population in East African countries continues to rise, we predict that spam from these countries, such as Kenya will increase with up to twice as much spam in 2011 as in 2010 driven by botnet domination. Spam sent from Africa will account for almost 5% of all spam by the end of 2011.

Contributions to the global spam landscape will also continue to shift geographically. The amount of spam sent from European countries will increase to 40-45% of all spam. Much of the shift will be due to an increase in spam from Eastern European countries, from the current 50% of spam from Europe to more than 70% in 2011. Spam sent from South America will account for 10-15% of all spam. North America will remain on par with around 10% of spam sent from the region, and Asia will remain relatively unchanged with around 35% of spam sent from the region.

Distributed Workforce Drives Security Policies

The past year has challenged businesses with securing an increasingly distributed workforce in the wake of the recent global economic crisis. With laptops and smart-phones becoming ubiquitous the workforce is increasingly distributed regardless of where workers spend their traditional work day. To remain competitive, as the economy begins to recover, companies will continue to look to employee productivity gains from longer hours, working remotely and from home offices. IDC estimates that one billion workers will be mobile at least part of the time or remote from their firm's main location by the end of 2011. These workers will be accessing business applications across a number of different devices.

In 2011, businesses will become more aware of the issues associated with managing remote workers and recognize the need to apply consistent policy controls and safeguard Internet access from malware such as that from unsecured USB storage devices, and drive-by attacks on compromised web sites.

Security and Services Continue Migrate to the Cloud

An increasingly distributed workforce is pushing organizations to the cloud for suitable security solutions that will be required to work seamlessly across multiple platforms, as users switch between devices used to store and transmit information online. In 2011 businesses will increasingly begin to reap the benefits of adopting a hybrid infrastructure that is premise-based, private cloud-based and public cloud-based and will seek to deliver a seamless user experience regardless of device or access location.

Making Web Security Work in an Era of Pervasive Threats

In 2010 more than 80% of malicious threats intercepted were found on legitimate web sites that had been compromised either directly or indirectly via third party-provided content. At the same time categories which were once easy to block universally, like social media, are becoming increasingly business relevant.

In 2011 we expect IT managers will be forced by business necessity to implement more granular and refined web security policies. Particular business units, departments or users will be granted access to certain web sites or categories of sites. MessageLabs Intelligence data indicates that the number of custom policy rules will increase from approximately 30 to more than 50 per organization to achieve a more granular response to web filtering. Also, default policies will become more nuanced, industry-specific and business role-specific to ease the burden on IT managers.

Stuxnet Strikes Up Malware Specialization

One of the most threatening advances in malware during 2010 broadened the range of targets beyond PCs and servers when the Stuxnet Trojan attacked programmable logic controllers. This specialized malware written to exploit physical infrastructures will continue in 2011 driven by the huge sums of money available to criminal enterprises at low risk of prosecution.

These attacks will range from the obvious targets like smart phones, to any number of less obvious yet critical systems like power grid controls or electronic voting systems. Any technology that can be exploited for financial gain or influence will become a potential target.

Trending Topics Fashioned to Follow the News

We've seen malware that attempts to ensure that links to infected pages are returned in search engine results using black hat search engine optimization techniques.

In 2011, the criminals will go one step further. Rather than just promoting compromised web sites through search engine optimization they will proactively identify web sites likely to see higher than normal levels of traffic based on current events or hot topics on the internet. They will use multiple methods, including monitoring of micro-blogging site topics and search engine hot topic feeds to track these trending topics. Combined with an understanding of potential site vulnerabilities this information can be used to compromise appropriate target sites quickly enough to exploit expected surges in traffic.

Automation Advances Targeted Attacks

Highly targeted attacks are steadily increasing in number. These carefully crafted attacks target specific users in specific organizations and require significant effort and research on behalf of the cyber criminal.

In 2011 criminal enterprises will increasingly automate this research to create a heavier volume of more powerful and convincing attacks that appear particularly relevant, interesting and/or newsworthy to the intended victims.

Botnets Evolve with Steganography

Since the McColo ISP takedown in November 2008, which removed the command and control servers used by cyber crooks to control the activities of their botnets, and wiped out many cyber crime operations, the cyber criminals have been looking to build business continuity practices into their operations.

In 2011, we expect that botnet controllers will resort to employing steganography techniques to control their computers. This means hiding their commands in plain view – perhaps within images or music files distributed through file sharing or social networking web sites. This approach will allow criminals to surreptitiously issue instructions to their botnets without relying on an ISP to host their infrastructure thus minimizing the chances of discovery.

Rogue Marketplace Vendors Exploit Online Digital Currencies

In 2011 social networking sites and online marketplaces will roll out their own in-house digital virtual currencies. As an example, one social networking site already has a system in place that uses "Credits." Attacks will soon be designed to seek to exploit these new areas for financial fraud, including specialized malware, rogue applications and phishing attacks.

We expect more social networking environments and online marketplaces will move toward adopting this approach, and that these systems will come under prolonged attack where a weakness in one will be identified as the target in a mainstream malware attack or phishing scam in 2011. These currencies will also be exploited as a means of transferring ill gotten gains outside of national and international banking regulatory and anti-laundering regimes.

Hackers Exploit Router Vulnerabilities

As 2010 has proven there are many systems vulnerable to attack. We often focus on PCs, servers and devices but recently it has become apparent that routers are also open to exploit. Router vulnerabilities, allow attackers to re-route network traffic with malicious intent. As an example, a user could be diverted from an online banking site to an identical malicious web site and their login credentials could be stolen or a business user could be diverted from a legitimate CRM, ERP or HR service allowing a hacker to access client, business or staff information. When properly structured, these attacks can forward the user to the legitimate site with no indication the attack has occurred.

In 2011, we expect to uncover new variants of malware that will include functionality to actively search for and exploit business and home networking hardware with known vulnerabilities. Since networking equipment software and firmware is rarely updated these vulnerabilities can exist for years.

Cyber Criminals Usurp URL Shortening Services

URL shortening services are becoming critical to the operation of social networks, particularly those that apply a character limit to user updates. In 2010 we saw a number of exploits using URL shortening services that lead to compromised sites.

In 2011 we expect to see more sophisticated attacks using URL shortening services either by a criminal enterprise gaining control of a significant URL shortening service or one of these groups setting up a service which appears legitimate, and operates in a legitimate manner, before being turned to malicious use. Even occasional malicious use cloaked within a legitimate service or legitimate-looking service could prove very effective.

Targeted Attacks Diversify

Targeted attacks remain a significant risk. While the volume of these attacks is low relative to mass spam and malware attacks they are very effective in bypassing all traditional security systems and user training. In 2010 cyber criminals began honing in on industries not previously targeted. At one point 25% of attacks were against the retail sector which had previously seen few to no targeted attacks.

In 2011, we expect the range of organizations being targeted in such attacks to become more diverse. This means that attackers will also seek indirect entry into specific industries by exploiting contractors and suppliers, rather than directly targeting only the executives in each industry sector.

10 CONTRIBUTORS

Paul Wood
Executive Editor &
Senior Analyst

Martin Lee
Senior Software Engineer

Dan Bleaken
Senior Malware Data Analyst

Mat Nisbet
Malware Data Analyst

Yuriko Kako-Batt
Internet Data Analyst

Nicholas Johnston
Senior Anti-Spam Engineer

Anoirel Issa
Malware Analyst

Bhaskar Krishnappa
Malware Analyst

Manoj Venugopalan
Malware Analyst

Jo Hurcombe
Anti-Virus Operations Engineer

Marissa Vicario
Corporate Communications

Daren Lewis
Corporate Communications

MessageLabs Intelligence
Symantec's MessageLabs Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. MessageLabs Intelligence provides a range of information on global security threats based on live data feeds from our control towers around the world scanning billions of messages each week. All MessageLabs Intelligence reports and analysis 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.