Symantec Intelligence

Symantec Intelligence Report: July 2011

Aggressive use of rapidly changing malware leads to a rise in sophisticated socially engineered attacks; twist in phishing attacks bait mobile phone users

Welcome to the July edition of the Symantec Intelligence report, now combining the best research and analysis from the Symantec.cloud MessageLabs Intelligence Report and the Symantec State of Spam & Phishing Report, providing the latest analysis of cyber security threats, trends and insights from the Symantec Intelligence team concerning malware, spam, and other potentially harmful business risks. The data used to compile the analysis for this combined report includes data from June and July 2011.

Report highlights

- Spam – 77.8 percent in July (an increase of 4.9 percentage points since June 2011): page 9
- Phishing – One in 319.3 emails identified as phishing (an increase of 0.01 percentage points since June 2011): page 12
- Malware – One in 280.9 emails in July contained malware (an increase of 0.02 percentage points since June 2011): page 13
- Malicious Web sites – 6,797 Web sites blocked per day (an increase of 25.5 percent since June 2011): page 15
- 35.9 percent of all malicious domains blocked were new in July (an increase of 0.8 percentage points since June 2011): page 15
- 21.1 percent of all Web-based malware blocked was new in July (an increase of 0.8 percentage points since June 2011): page 15
- Aggressively unstable malware leads to a rise in sophisticated socially engineered attacks: page 2
- Phishers' World in Your Cell Phone: page 6
- Large scale malware attack using URL shortening services: page 7
- Best Practices for Enterprises and Users: page 18

Introduction

With one in 280.9 emails identified as malicious in July, further analysis reveals a significant increase in activity related to what may be described as an aggressive and rapidly changing form of generic polymorphic[1] malware. This rise accounted for 23.7 percent of all email-borne malware intercepted in July; more than double the same figure six months ago, indicating a much more aggressive strategy on the part of the cyber criminals responsible, perhaps greater use of automation has enabled them to increase their output to this extent.

In the same time frame, the number of variants, or different strains of malware involved in each attack has also grown dramatically by a factor of 25 times the same quantity six months previously; an alarming proliferation in such a short time almost certainly heightens the risk profiles of many organizations as these new strains are much harder to detect using traditional security defenses. This new breed of malware is likely to be causing a great deal of pain for a great number of traditional anti-virus companies that rely on signatures, heuristics and software emulation in order to detect malicious activity.

The malware is frequently contained inside an executable within the attached ZIP archive file and often disguised as a PDF file or an office document. This new aggressive approach to distributing generic polymorphic malware on such a scale should be concerning for many businesses, particularly for those who rely solely on more traditional security countermeasures, which this type of malware is designed to evade. One example of this technique involves changing the startup code in almost every version of the malware; subtly changing the structure of the code and making it

[1] *Polymorphic malware may have many variations of the same code using different encoding techniques, but the functionality of the program remains the same in each version*

harder for emulators built-in to many anti-virus products to identify the code as malicious. Technology cannot rely on signatures and heuristics alone, and must also take into account the integrity of an executable based on knowledge of its reputation and circulation in the real-world.

In other news, phishing attacks have also been seeking various means to exploit vulnerable cell phone users; two key areas in which we can see this trend are, firstly, the increase in phishing against wireless application protocol (WAP) pages, which are lightweight Web pages designed for smaller mobile devices such as cell phones; and secondly, the use of compromised domain names that have been registered for mobile devices, for example, using the .mobi top-level domain. Symantec has identified phishing sites spoofing such Web pages and has been monitoring the trend. In July, social networking and information services brands were frequently observed in these phishing sites. The primary motive of these attacks continues to be identity theft. Targeting cell phone users is just part of a new strategy for achieving the same result.

I hope you enjoy reading this month’s edition of the report, and please feel free to contact me directly with any comments or feedback as to what you like or dislike about the new format.

Paul Wood, Senior Intelligence Analyst
paul_wood@symantec.com
@paulowoody

Report analysis

Aggressively unstable malware leads to a rise in sophisticated socially engineered attacks

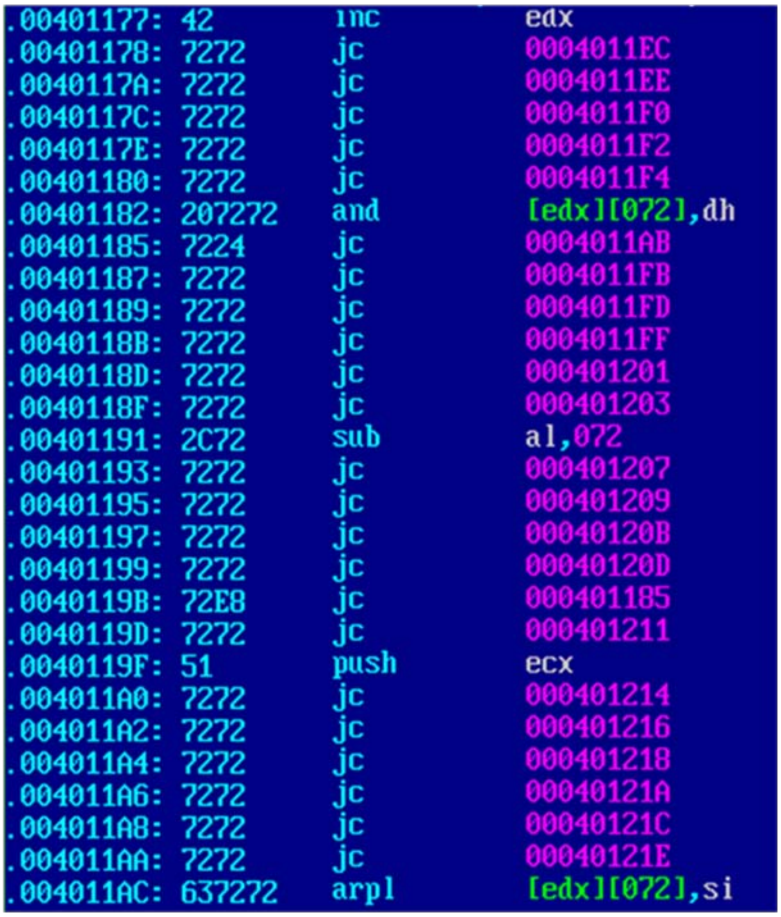
With one in 280.9 emails identified as malicious in July, further analysis reveals a significant increase in activity related to what may be described as an aggressively unstable or rapidly changing form of generic polymorphic malware. This rise accounted for 23.7 percent of all email-borne malware intercepted in July. The malware is frequently contained inside an executable within the attached ZIP archive file, sometimes disguised as a PDF file, for example.

In February,[2] we first reported a rise in synchronized, integrated malicious attacks involving a number of different strains of generic polymorphic malware, including Bredolab, Zeus, Zbot and SpyEye. Over the course of the following months the level of activity related to this pattern of malicious activity has continued to increase. In February, generic polymorphic malware accounted for approximately 10.3 percent of all email-borne malware, doubling to 23.7 percent in July. This is an alarming proliferation in such a short time and almost certainly heightens the risk profile of many organizations confronted with this threat.

These new strains are much harder to detect using traditional security defenses and this new breed of malware is potentially causing a great deal of pain for many traditional anti-virus companies that often rely on signatures, heuristics and software emulation in order to detect malicious activity.

Further analysis shows that the most recent samples were specifically designed to evade detection by software emulators that often form part of the anti-virus engine installed on a target PC. Software emulation is designed to analyze the code and follow the flow of instructions, but only up to a point. One design element of this new breed of malware includes a series of unnecessary “jump” instructions in the startup code, which are introduced in between the real instructions specifically to confound the anti-virus engine detection. An example of this can be seen in figure 1, where every instruction has around 5 or 6 extra jumps that add nothing to the actual functionality of the code.

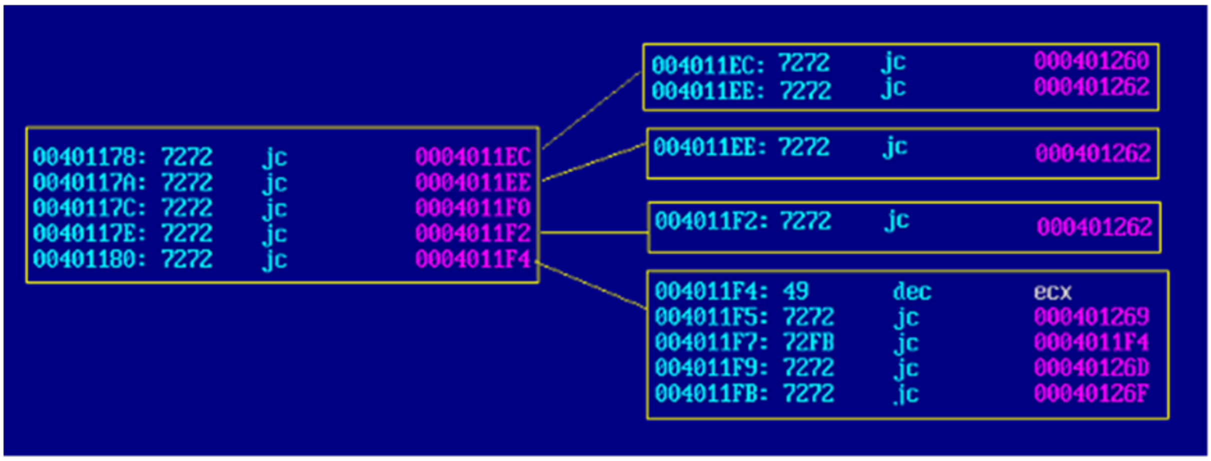
[2] http://www.symanteccloud.com/mlireport/MLI_2011_02_February_FINAL-en.PDF



```
.00401177: 42         inc     edx
.00401178: 7272       jc      0004011EC
.0040117A: 7272       jc      0004011EE
.0040117C: 7272       jc      0004011F0
.0040117E: 7272       jc      0004011F2
.00401180: 7272       jc      0004011F4
.00401182: 207272     and     [edx][072],dh
.00401185: 7224       jc      0004011AB
.00401187: 7272       jc      0004011FB
.00401189: 7272       jc      0004011FD
.0040118B: 7272       jc      0004011FF
.0040118D: 7272       jc      000401201
.0040118F: 7272       jc      000401203
.00401191: 2C72       sub     al,072
.00401193: 7272       jc      000401207
.00401195: 7272       jc      000401209
.00401197: 7272       jc      00040120B
.00401199: 7272       jc      00040120D
.0040119B: 72E8       jc      000401185
.0040119D: 7272       jc      000401211
.0040119F: 51         push    ecx
.004011A0: 7272       jc      000401214
.004011A2: 7272       jc      000401216
.004011A4: 7272       jc      000401218
.004011A6: 7272       jc      00040121A
.004011A8: 7272       jc      00040121C
.004011AA: 7272       jc      00040121E
.004011AC: 637272     arpl    [edx][072],si
```

Figure 1: Fragment of startup code illustrating surplus jump (JC) instructions between code

Furthermore, these jump instructions often lead to other jump instructions, as shown in figure 2, hence this technique is not only able to evade traditional anti-virus signatures, but this can even break the emulation techniques used in anti-virus engines by introducing more junk instructions in between the valid instructions.



```
00401178: 7272     jc     0004011EC
0040117A: 7272     jc     0004011EE
0040117C: 7272     jc     0004011F0
0040117E: 7272     jc     0004011F2
00401180: 7272     jc     0004011F4
```

```
004011EC: 7272     jc     000401260
004011EE: 7272     jc     000401262
```

```
004011EE: 7272     jc     000401262
```

```
004011F2: 7272     jc     000401262
```

```
004011F4: 49       dec    ecx
004011F5: 7272     jc     000401269
004011F7: 72FB     jc     0004011F4
004011F9: 7272     jc     00040126D
004011FB: 7272     jc     00040126F
```

Figure 2: Schematic showing how program passes control through a series of additional jumps

The largest spikes of this activity since 10 June occurred around the dates of 18 June, 28 June and 7 July; as can be seen in figure 3.

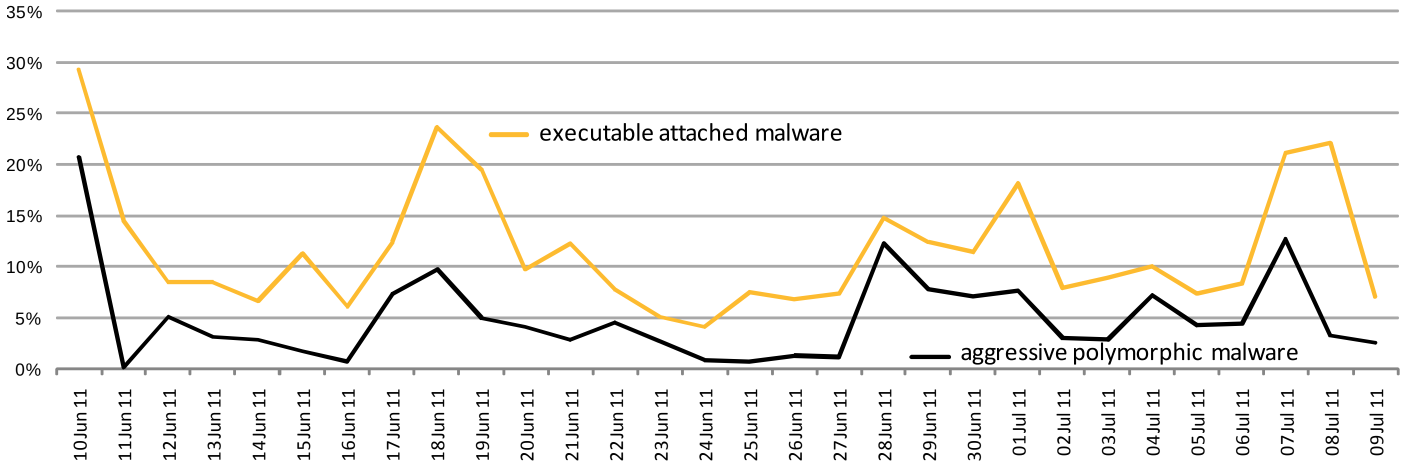
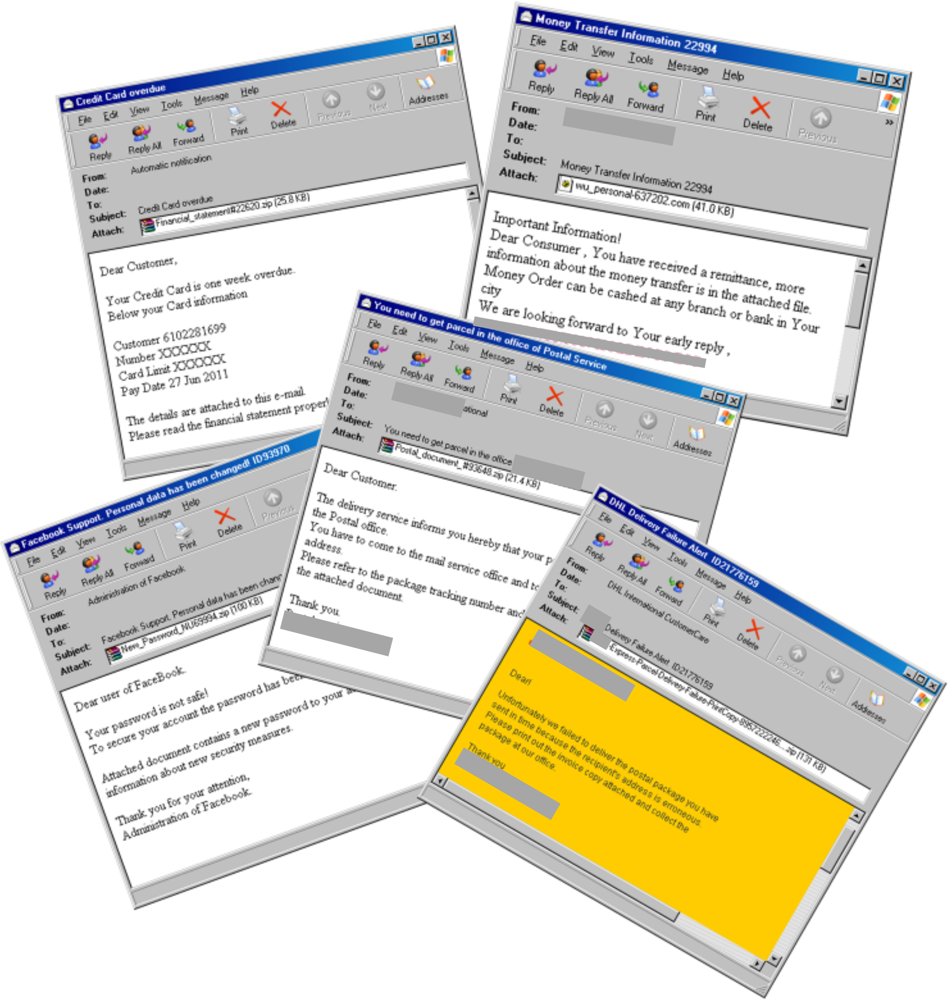


Figure 3: Chart showing pattern of generic polymorphic malware and executable attachment malware

For the entire period between June and July highlighted in figure 3 above, approximately 11.1 percent of all email-borne malware intercepted was identified as malicious, executable attachments, of which 46.0 percent could be classified as aggressively unstable polymorphic malware. During this period, Symantec Intelligence identified approximately 1,057 different strains of generic polymorphic malware being blocked, approximately 25 times more than in February 2011, when approximately 40 strains were identified. This indicates a much more aggressive strategy on the part of the cyber criminals responsible, perhaps greater use of automation has enabled them to increase their output to this extent. Such an alarming proliferation in only six months almost certainly heightens the risk profile of many organizations as these new strains are much harder to detect using traditional security defenses.

Many of these involved dictionary attacks, where the recipient names are often generated automatically using dictionaries of first and last names. Dictionary attacks often result in a large number of Non-Delivery Reports (NDRs) where emails sent to invalid addresses often result in emails being bounced as undeliverable. This pattern can be clearly seen in the section on Spam Attack Vectors (page 11), later in this report.

Examples of these recent email-borne attacks can be seen in figure 4, below. Although some of the more recent attacks have spoofed credit-card providers, suggesting the recipient is overdue in settling their balance.



File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

Credit Card overdue

From: Automatic notification
Date:
To:
Subject: Credit Card overdue
Attach: Financial_statement#22620.zip (25.8 KB)

Dear Customer,

Your Credit Card is one week overdue.
Below your Card information

Customer 6102281699
Number XXXXXX
Card Limit XXXXXX
Pay Date 27 Jun 2011

The details are attached to this e-mail.
Please read the financial statement propert

Money Transfer Information 22994

From: [redacted]
Date:
To:
Subject: Money Transfer Information 22994
Attach: wu_personal-637202.com (41.0 KB)

Important Information!
Dear Consumer , You have received a remittance, more information about the money transfer is in the attached file.
Money Order can be cashed at any branch or bank in Your city
We are looking forward to Your early reply ,
[redacted]

You need to get parcel in the office of Postal Service

From: [redacted]ational
Date:
To:
Subject: You need to get parcel in the office [redacted]
Attach: Postal_document_#93648.zip (21.4 KB)

Dear Customer.

The delivery service informs you hereby that your p
the Postal office.
You have to come to the mail service office and to
address.
Please refer to the package tracking number and
the attached document.

Thank you.
[redacted]

Facebook Support. Personal data has been changed! ID93970

From: Administration of Facebook
Date:
To:
Subject: Facebook Support. Personal data has been chang
Attach: New_Password_NU69994.zip (100 KB)

Dear user of FaceBook.

Your password is not safe!
To secure your account the password has bee

Attached document contains a new password to your
information about new security measures.

Thank you for your attention,
Administration of Facebook.

DHL Delivery Failure Alert ID21776159

From: DHL International CustomerCare
Date:
To: [redacted]
Subject: Delivery Failure Alert ID21776159
Attach: Express-Parcel-Delivery-Failure-PrintCopy-8957222246....zip (131 KB)

[redacted]

Dear

Unfortunately we failed to deliver the postal package you have sent in time because the recipient's address is erroneous.
Please print out the invoice copy attached and collect the package at our office.

Thank you
[redacted]

Figure 4: Examples of recent malware attacks using aggressive polymorphic techniques

As can be seen in figure 5, the most common forms of these attacks are often disguised as correspondence from parcel carriers and courier-based delivery services.

Subject	Number Blocked in 24 Hours
Money Transfer	419
[redacted]	594
[redacted] Delivery Confirmation	1013

Figure 5: Examples of recent malware attacks using aggressive polymorphic techniques

On 18 July another wave of attacks further revealed the scale of the aggressive polymorphic nature of these attacks, when 52 strains were identified in approximately 2,816 attacks, as highlighted in figure 6, below.

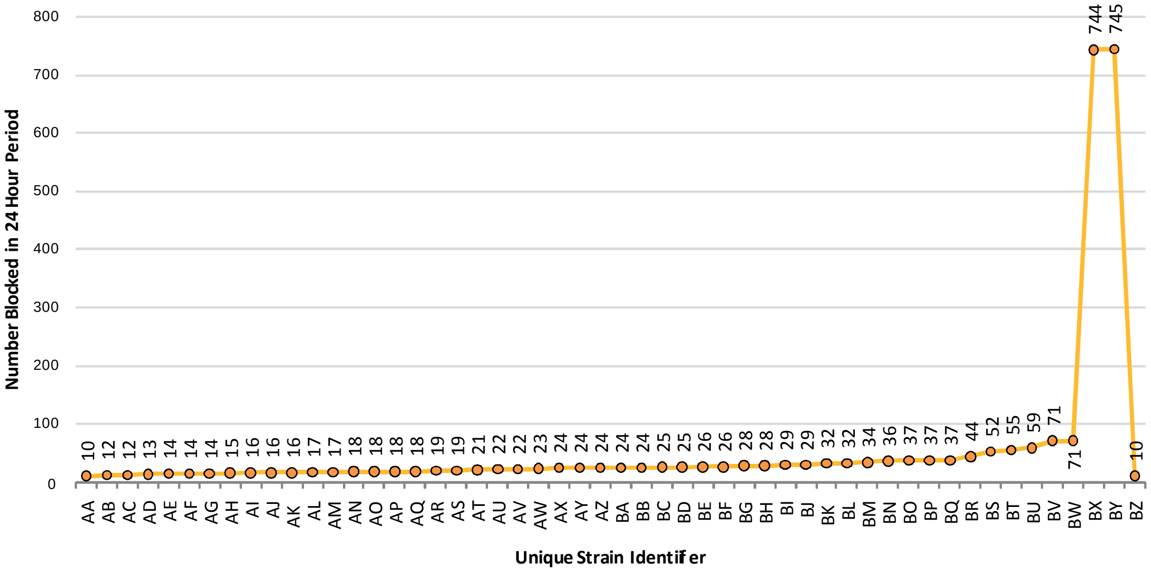


Figure 6: Chart showing number of copies intercepted of each new polymorphic strain on 18 July 2011

If the recipient opens the attached executable, the malware is injected into a running process before downloading further malware from the Internet. The Web sites used to retrieve the instructions and subsequent malware appear to be hosted on fast-flux domains. Fast-flux involves the use of continually changing IP addresses associated with the domain names involved. Often these IP addresses will belong to compromised computers perhaps hosted within the context of a wider botnet. By continually changing these IP addresses, the attackers can prevent the malware from spreading by disrupting the Web sites hosting it. In order to dismantle a fast-flux domain, the domain registrar must be notified of the malicious use of the service so that it may be taken offline and removed from the DNS registry.

This new aggressive approach to distributing generic polymorphic malware on such a scale is concerning for many businesses who rely solely on traditional security countermeasures, which this type of malware is designed to evade. Technology cannot rely on signatures and heuristics alone, and must also take account of the integrity of an executable based on knowledge of its reputation or circulation.

Phishers' World in Your Cell Phone

Technologies in cell phones are advancing day after day, and so phishers are also seeking various means to exploit vulnerable cell phone users. The two key areas in which we can see this trend are, firstly, the increase in phishing against wireless application protocol (WAP) pages, and secondly, the use of compromised domain names that have been registered for mobile devices.

Many legitimate brands have designed their websites for cell phones or WAP pages. The difference between a WAP page and a regular Web page is that the WAP page uses reduced file sizes and minimal graphics. This is done for cell phone compatibility and also to achieve higher browsing speeds while the user is on the move. Symantec has identified phishing sites spoofing such Web pages and has been monitoring the trend. In July, social networking and information services brands were frequently observed in these phishing sites.

In the example shown in figure 7 below, the phishing page consists of nothing more than a form asking for users' credentials (This is a typical design created for cell phones). When a victim enters the required information, the phishing page is redirected to the WAP page of the legitimate brand. The phishing site in this case was hosted on a free Web hosting site.

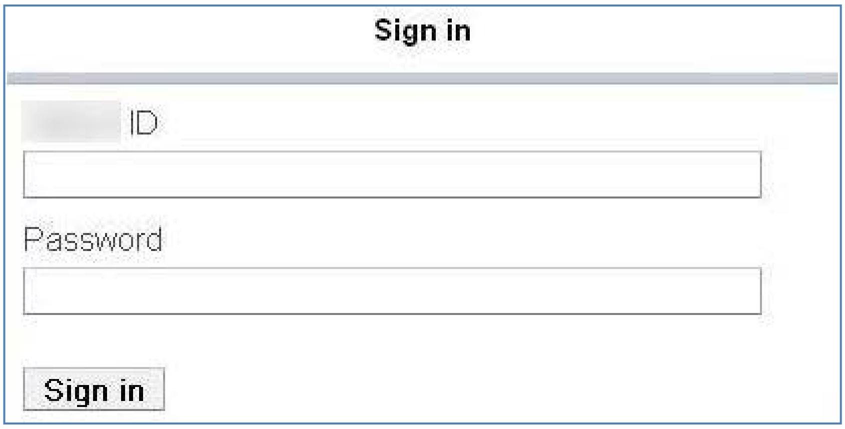


Figure 7: Example phishing page requesting users' credentials

The domain names used for websites accessed by mobiles devices commonly have a ".mobi" top level domain (TLD). These domain names are compromised and utilized by phishers to host several phishing sites. Over the past six months, about 65 percent of these phishing sites spoofed brands from the banking sector, whereas 19 percent were from the e-commerce sector and the remaining were from the ISP, social networking, and information services sectors.

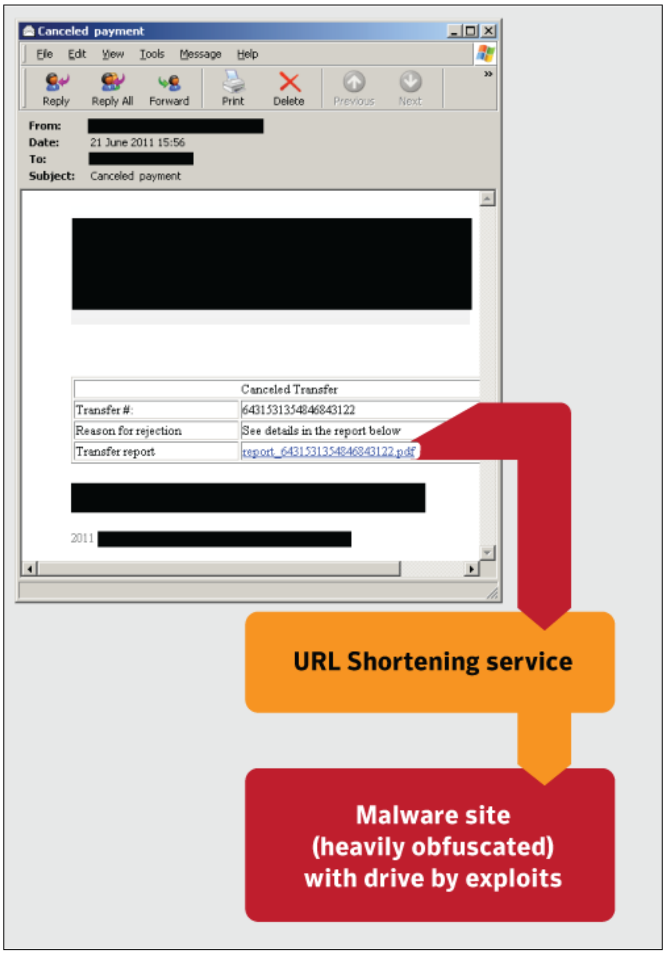
The primary motive of phishers in these attacks continues to be identity theft. Targeting cell phone users is just part of a new strategy for achieving the same result.

Large scale malware attack using URL shortening services

We've seen spammers abusing URL shortening services on a huge scale for quite some time, which was also reported in-depth as part of the May 2011 MessageLabs Intelligence Report [3]. The explosion in popularity of micro-blogging services and social networking status updates has seen a huge increase in the number of URL shortening sites. The simple and semi-anonymous nature of these sites allows spammers to easily create thousands of links which they then include in their spam in an attempt to evade URL-based spam blocking. In July Symantec Intelligence identified a large malware attack using URL shortening services.

The attack abused at least five different URL shortening sites. The message claimed to be from an inter-bank funds transfer service, claiming that a funds transfer had been cancelled. To find out why the transfer was cancelled, recipients were encouraged to click on a link supposedly pointing to a PDF file, but actually pointing to a shortened URL. This shortened URL then redirects to a site with several drive-by exploits. The process can be seen in figure 8, below.

[3] http://www.symanteccloud.com/mlireport/MLI_2011_05_May_FINAL-en.pdf



From: [redacted]
Date: 21 June 2011 15:56
To: [redacted]
Subject: Canceled payment

[redacted]

Canceled Transfer	
Transfer #:	6431531354846843122
Reason for rejection	See details in the report below
Transfer report	report_6431531354846843122.pdf

[redacted]

2011 [redacted]

Figure 8: Illustration of the process involved in URL shortening services and drive-by malware

The malware Web site was heavily obfuscated; almost its entire content is obfuscated and contained inside a single huge HTML "DIV" element, hidden with inline CSS. When a web browser renders the page, JavaScript is used to de-obfuscate the content and run more JavaScript to carry out exploits. The page attempts several exploits including exploits targeting PDF and Java, and also uses a Windows Help Center exploit to download more malware.

We saw hundreds of unique shortened URLs being used to link to this malware, and expect to see malware authors using this technique in future.

Global Trends & Content Analysis

Spam, phishing and malware data is captured through a variety of sources, including the Symantec Global Intelligence Network, the Symantec Probe Network (a system of more than 5 million decoy accounts), Symantec.cloud and a number of other Symantec security technologies. Skeptic™, the Symantec.cloud proprietary heuristic technology is also able to detect new and sophisticated targeted threats.

Data is collected from over 8 billion email messages and over 1 billion Web requests which are processed per day across 16 data centers, including malicious code data which is collected from over 130 million systems in 86 countries worldwide. Symantec intelligence also gathers phishing information through an extensive antifraud community of enterprises, security vendors, and more than 50 million consumers.

These resources give the Symantec Intelligence analysts unparalleled sources of data with which to identify, analyze, and provide informed commentary on emerging trends in attacks, malicious code activity, phishing, and spam. If there is a malicious attack about to hit, we know about it first. We block it; we keep it from affecting our customers.

Spam Analysis

In July 2011, the global ratio of spam in email traffic rose to 77.8 percent (1 in 1.29 emails); an increase of 4.9 percent when compared with June 2011.

Spam Rate

77.8%

Last Month:	72.9%
Six Month Avg.:	76.7%

Top 5 Geographies

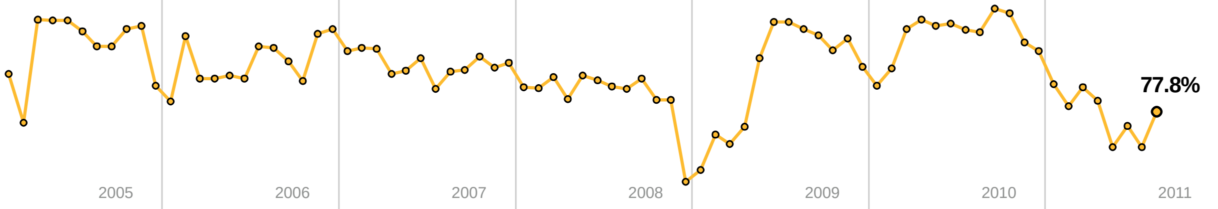
85.6%	Saudi Arabia
83.4%	Russian Federation
82.4%	China
81.9%	Hungary
81.6%	Viet Nam

Top 5 Verticals

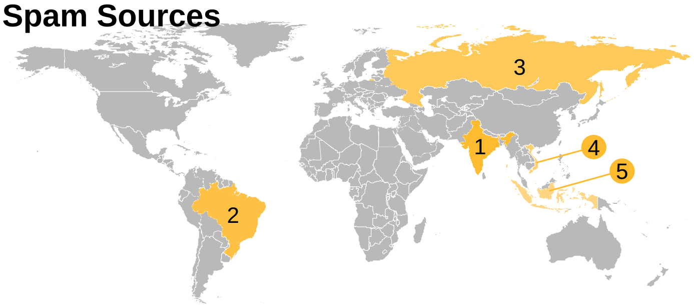
80.7%	Automotive
80.3%	Education
79.2%	Marketing/Media
79.1%	Manufacturing
78.8%	Accom/Catering

By Horizontal

77.4%	1-250
77.5%	251-500
78.0%	501-1000
78.5%	1001-1500
78.3%	1501-2500
77.9%	2501+



Spam Sources



India	15.5%
Brazil	13.1%
Russian Federation	6.4%
Viet Nam	6.4%
Indonesia	2.6%
China	2.5%
Ukraine	2.4%
Romania	2.4%
Saudi Arabia	2.4%
United States	2.3%

July 2011

As the global spam level declined in July 2011, Saudi Arabia remained the most spammed geography, with a spam rate of 85.6 percent, and Russia remained the second most-spammed.

In the US, 78.0 percent of email was spam and 77.7 percent in Canada. The spam level in the UK was 78.2 percent. In The Netherlands, spam accounted for 78.8 percent of email traffic, 77.9 percent in Germany, 77.6 percent in Denmark and 75.8 percent in Australia. In Hong Kong, 76.8 percent of email was blocked as spam and 75.7 percent in Singapore, compared with 74.7 percent in Japan. Spam accounted for 76.9 percent of email traffic in South Africa and 78.7 percent in Brazil.

In July, the Automotive industry sector remained the most spammed industry sector, with a spam rate of 80.7 percent. Spam levels for the Education sector reached 80.3 percent and 77.9 percent for the Chemical & Pharmaceutical sector; 77.8 percent for IT Services, 77.8 percent for Retail, 77.0 percent for Public Sector and 77.0 percent for Finance.

Global Spam Categories

The most common category of spam in July was pharmaceutical related, but the second most common was related to adult/dating spam. Examples of many of these subjects can be found in the subject line analysis, below.

Category Name	June 2011	July 2011
Pharmaceutical	40.0%	47.0%
Adult/Sex/Dating	19.0%	14.5%
Jobs/Recruitments	-	10.5%
Watches/Jewelry	17.5%	7.5%
Unsolicited Newsletters	11.5%	7.5%
Casino/Gambling	7.0%	3.5%
Degrees/Diplomas	1.5%	2.5%
Unknown/Other	2.5%	2.0%

Spam Subject Line Analysis

In the latest analysis, adult-related dating spam dominates the top spam subject line list in July. .

Rank	Total Spam: June 2011 Top Subject Lines	No. of Days	Total Spam: July 2011 Top Subject Lines	No. of Days
1	*Blank Subject line*	31	drop me a line	31
2	*Re: Windows 7, Office 2010, Adobe CS5 …*	16	r u online now?	16
3	*im online now*	31	hi darling..	31
4	*my new pics :)*	31	new email	31
5	*drop me a line*	31	found you :)	31
6	*r u online now?*	31	im online now	31
7	*hi darling..*	31	my new pics :)	31
8	*new email*	31	my new email	31
9	*found you :)*	31	my hot pics :)	31
10	*my hot pics :)*	31	I'm online now…	31

Spam URL TLD Distribution

The proportion of spam exploiting URLs in the .RU top-level fell by 8.6 percentage points in July, with the largest increase relating to spam URLs in the .info TLD.

TLD	June	July	Change (% points)
com	53.4%	54.9%	+0.5
ru	19.2%	10.6%	-8.6
info	14.9%	18.3%	+3.4
net	5.5%	6.2%	+0.7

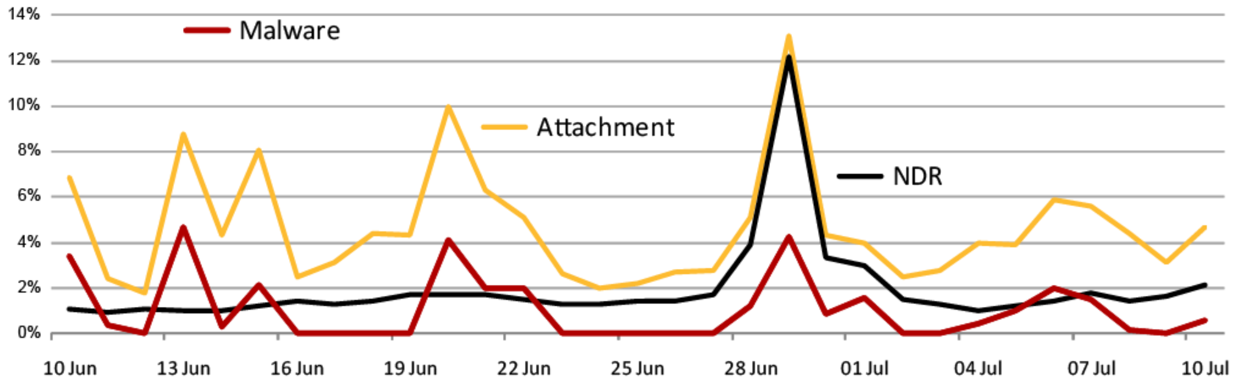
Average Spam Message Size

In July, almost two-thirds of spam was approximately 5Kb in size or less.

Message Size	June	July	Change (% points)
0Kb – 5Kb	62.3%	65.1%	+2.8
5Kb – 10Kb	24.2%	21.2%	-3.0
>10Kb	13.4%	13.7%	+0.3

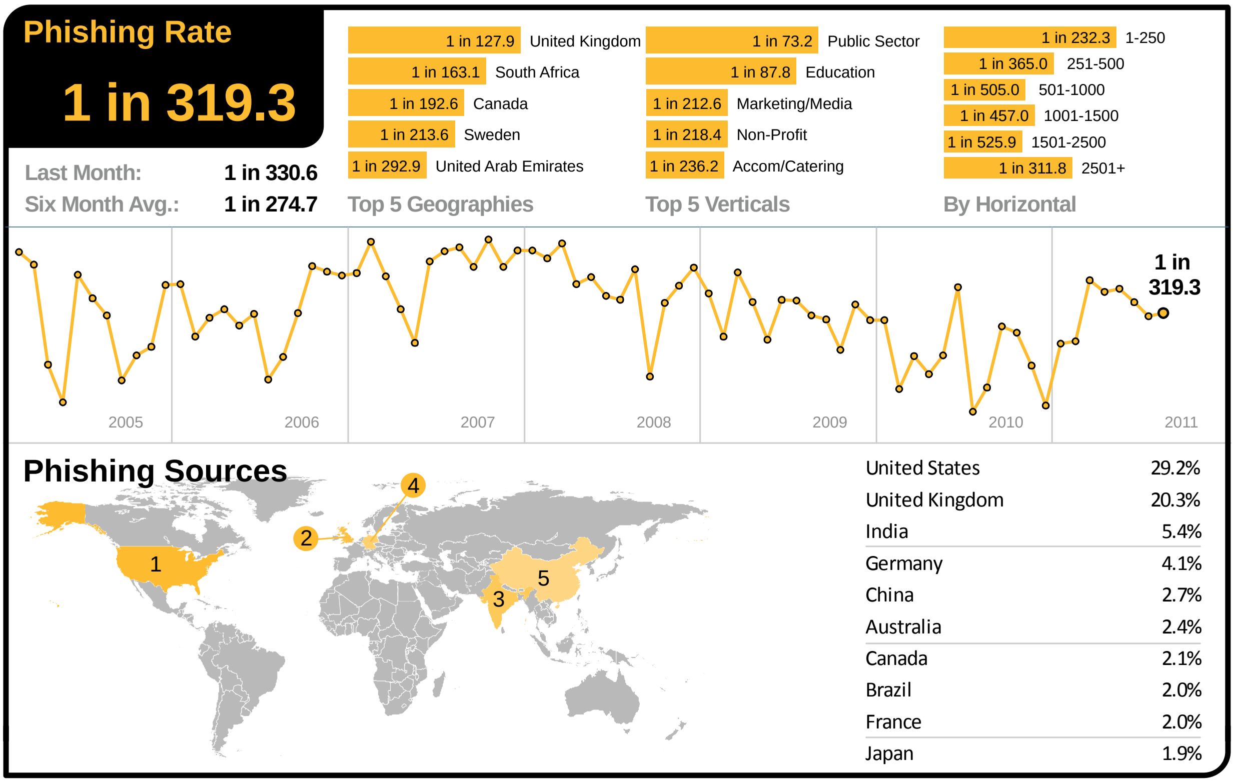
Spam Attack Vectors

It can be seen in the chart below that a major spike in attachment spam occurred on 29 June. This also coincided with a surge in NDR spam (spam related non-delivery reports). Further analysis of the latter indicated that dictionary attacks were used in order to send large volumes of spam containing attachments. The growth in attachments was also connected to a large volume of generic polymorphic malware being spammed-out on that date, as reported earlier in the report.



Phishing Analysis

In July, phishing email activity increased by 0.01 percentage points since June 2011; one in 319.3 emails (0.313 percent) comprised some form of phishing attack.



Last Month:	1 in 330.6
Six Month Avg.:	1 in 274.7

Top 5 Geographies

1 in 127.9	United Kingdom
1 in 163.1	South Africa
1 in 192.6	Canada
1 in 213.6	Sweden
1 in 292.9	United Arab Emirates

Top 5 Verticals

1 in 73.2	Public Sector
1 in 87.8	Education
1 in 212.6	Marketing/Media
1 in 218.4	Non-Profit
1 in 236.2	Accom/Catering

By Horizontal

1 in 232.3	1-250
1 in 365.0	251-500
1 in 505.0	501-1000
1 in 457.0	1001-1500
1 in 525.9	1501-2500
1 in 311.8	2501+

United States	29.2%
United Kingdom	20.3%
India	5.4%
Germany	4.1%
China	2.7%
Australia	2.4%
Canada	2.1%
Brazil	2.0%
France	2.0%
Japan	1.9%

July 2011

Phishing attacks in the UK increased to overtake South Africa and become the most targeted geography for phishing emails in July, with one in 127.9 emails identified as phishing attacks. Phishing in South Africa fell slightly to make it the second most targeted country, with one in 163.1 emails identified as phishing attacks.

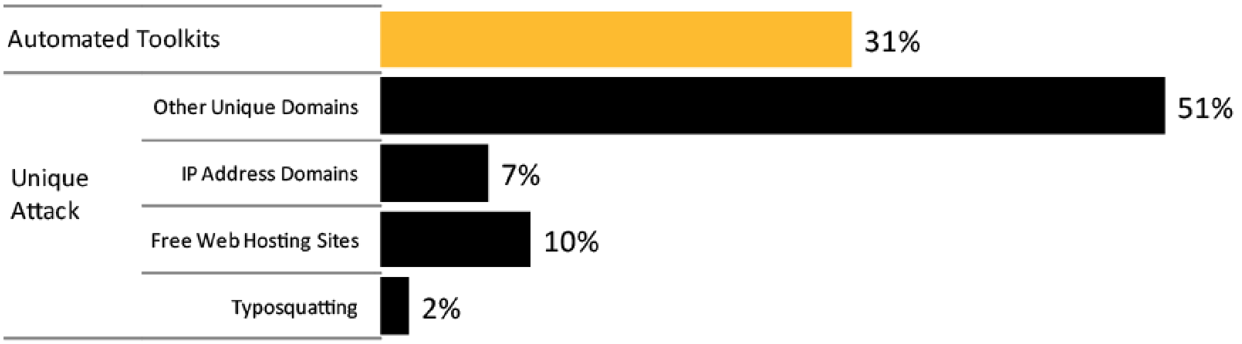
Phishing levels for the US were one in 1,237 and one in 192.6 for Canada. In Germany phishing levels were one in 798.3, one in 1,448 in Denmark and one in 526.9 in The Netherlands. In Australia, phishing activity accounted for one in 850.8 emails and one in 2,503 in Hong Kong; for Japan it was one in 13,167 and one in 872.9 for Singapore. In Brazil, one in 382.4 emails were blocked as phishing attacks.

The Public Sector remained the most targeted by phishing activity in July, with one in 73.2 emails comprising a phishing attack. Phishing levels for the Chemical & Pharmaceutical sector were one in 799.0 and one in 566.2 for the IT Services sector; one in 482.3 for Retail, one in 87.8 for Education and one in 396.7 for Finance.

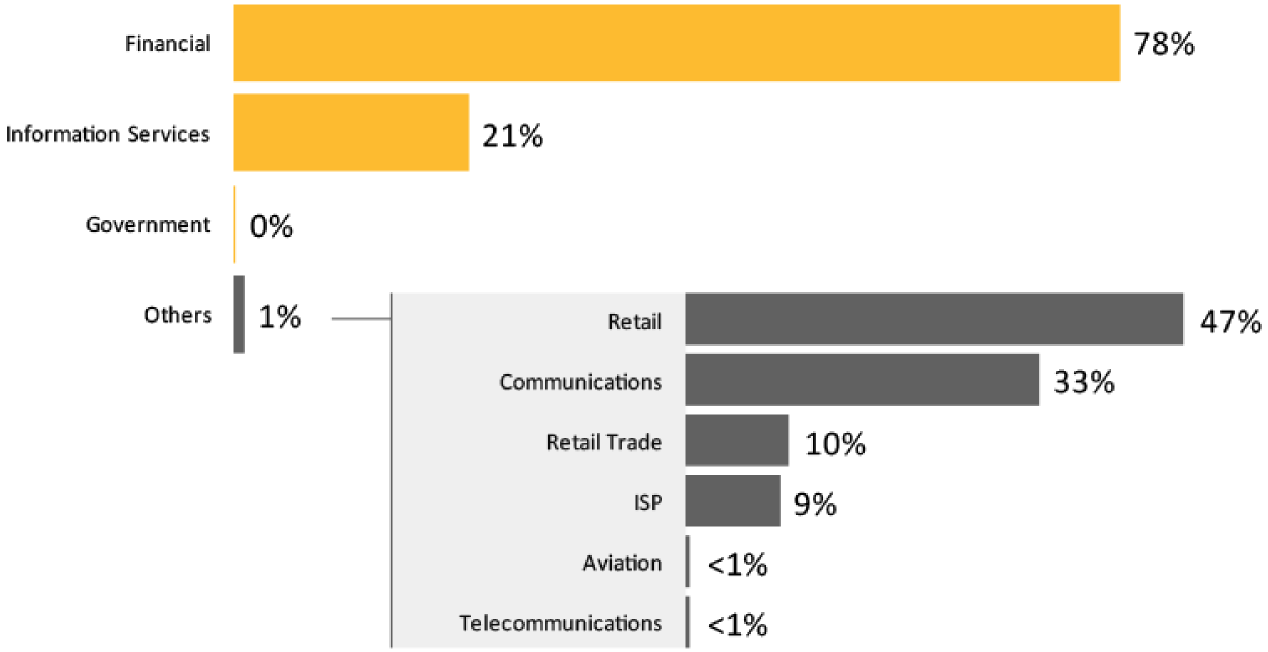
Analysis of Phishing Websites

The number of phishing Web sites decreased by 6.76 percent in July. Automated toolkit and unique domains decreased as compared to the previous month. The number of phishing websites created by automated toolkits decreased by about 6.50 percent. The number of unique phishing URLs also decreased by 6.87 percent and phishing websites using IP addresses in place of domain names (for example, http://255.255.255.255), increased by 58.5 percent. The use of legitimate Web services for hosting phishing Web sites accounted for approximately 10 percent of all phishing Web sites, a decrease of 1.6 percent from the previous month. The number of non-English phishing sites saw an increase of 9.1 percent. The most common non-English languages identified in phishing Web sites during July included Portuguese, French, Italian and Spanish.

Tactics of Phishing Distribution



Organizations Spoofed in Phishing Attacks, by Industry Sector

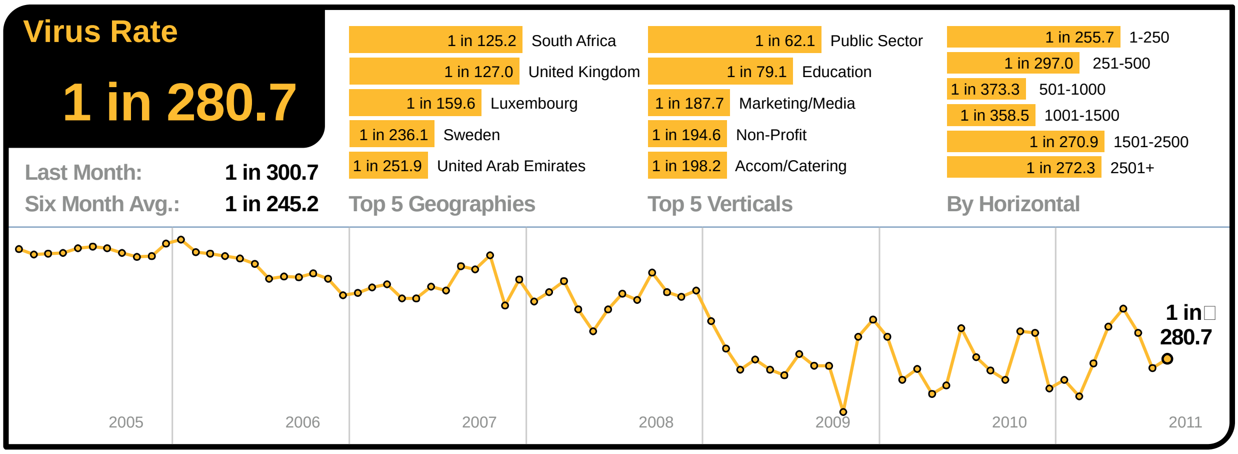


Malware Analysis

Email-borne Threats

The global ratio of email-borne viruses in email traffic was one in 280.9 emails (0.333 percent) in July, an increase of 0.01 percentage points since June 2011.

In July, 44.7 percent of email-borne malware contained links to malicious Web sites, a decrease of 2.0 percentage points since June 2011. A large number of emails contained generic polymorphic malware variants and accounted for 23.7 percent of all email-borne malware in July. Many variants of which were commonly attached as ZIP files, rather than hyperlinks, and as the volume of these attacks increased when compared with the previous month, the relative proportion of attacks using hyperlinks diminished



July 2011

Email-borne malware attacks rose in South Africa as the country became the geography with the highest ratio of malicious emails in July, overtaking the UK as one in 125.2 emails was identified as malicious in July; in the UK one in 127.0 emails was malicious. Whilst malicious activity increased in the UK and other countries, the increase was much more pronounced in South Africa owing to a sharp rise in the number of attacks related to the latest strains of aggressive polymorphic malware.

In the US, virus levels for email-borne malware were one in 634.8 and one in 255.9 for Canada. In Germany virus activity reached one in 482.1, one in 1,033 in Denmark and in The Netherlands one in 451.3. In Australia, one in 654.8 emails were malicious and one in 748.7 in Hong Kong; for Japan it was one in 2,093, compared with one in 761.8 in Singapore. In Brazil, one in 332.1 emails in contained malicious content.

With one in 62.1 emails being blocked as malicious, the Public Sector remained the most targeted industry in July. Virus levels for the Chemical & Pharmaceutical sector were one in 438.9 and one in 390.0 for the IT Services sector; one in 418.3 for Retail, one in 79.1 for Education and one in 443.5 for Finance.

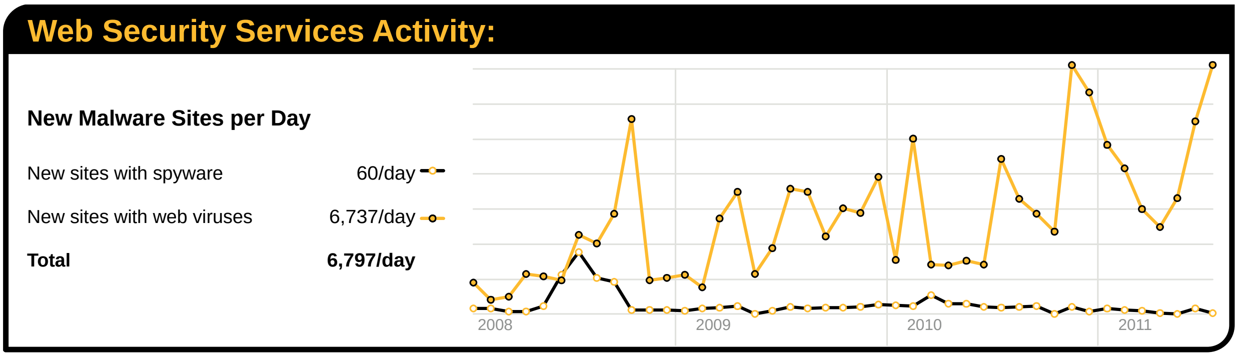
The table below shows the most frequently blocked email-borne malware for July, many of which take advantage of malicious hyperlinks. Overall, 23.7.0 percent of email-borne malware was associated with variants of generic polymorphic malware, including Bredolab, Sasfis, SpyEye and Zeus variants.

Malware Name	% Malware
W32/Bredolab.gen!eml	3.9%
Gen:Trojan.Heur.FU.bqW	5.7%
W32/NewMalware!836b	2.3%
Exploit/Link-7707	2.2%
Exploit/Link-48cc	2.1%
Exploit/LinkAliasPostcard-b11e	1.9%
W32/Netsky.c-mm	1.6%
Exploit/LinkAliasPostcard-f837	1.5%
W32/Generic-bbc5-0e41	1.3%
Exploit/Link-ExeSpoof	1.2%

Web-based Malware Threats

In July, Symantec Intelligence identified an average of 6,797 Web sites each day harboring malware and other potentially unwanted programs including spyware and adware; an increase of 25.5 percent since June 2011. This reflects the rate at which Web sites are being compromised or created for the purpose of spreading malicious content. Often this number is higher when Web-based malware is in circulation for a longer period of time to widen its potential spread and increase its longevity.

As detection for Web-based malware increases, the number of new Web sites blocked decreases and the proportion of new malware begins to rise, but initially on fewer Web sites. Further analysis reveals that 35.9 percent of all malicious domains blocked were new in July; an increase of 0.8 percentage points compared with June 2011. Additionally, 21.1 percent of all Web-based malware blocked was new in July; an increase of 0.8 percentage points since the previous month.



The chart above shows the increase in the number of new spyware and adware Web sites blocked each day on average during July compared with the equivalent number of Web-based malware Web sites blocked each day.

Web Policy Risks from Inappropriate Use

The most common trigger for policy-based filtering applied by Symantec Web Security.cloud for its business clients was for the “Advertisements & Popups” category, which accounted for 44.3 percent of blocked Web activity in July. Web-based advertisements pose a potential risk though the use of “malvertisements,” or malicious advertisements. These may occur as the result of a legitimate online ad-provider being compromised and a banner ad being used to serve malware on an otherwise harmless Web site.

The second most frequently blocked traffic was categorized as Social Networking, accounting for 16.6 percent of URL-based filtering activity blocked, equivalent to one in every six Web sites blocked.

Many organizations allow access to social networking Web sites, but facilitate access logging so that usage patterns can be tracked and in some cases implement policies to only permit access at certain times of the day and block access at all other times. This information is often used to address performance management issues, perhaps in the event of lost productivity due to social networking abuse.

Activity related to Streaming Media policies resulted in 7.5 percent of URL-based filtering blocks in July. Streaming media is increasingly popular when there are major sporting events or high profile international news stories, which often result in an increased number of blocks, as businesses seek to preserve valuable bandwidth for other purposes. This rate is equivalent to one in every 13.4 Web sites blocked.

Web Security Services Activity:

Policy-Based Filtering		**Web Viruses and Trojans**		**Potentially Unwanted Programs**	
Advertisement and Popups	44.3%	Trojan.Gen	11.0%	PUP:Generic.168911	24.0%
Social Networking	16.6%	Dropped:Trojan.PWS.OnlineGames.KDVN	9.8%	PUP:Clkpotato!gen2	14.4%
Streaming Media	7.5%	Trojan:HTML/GIFrame.gen!B	8.0%	PUP:Generic.178280	13.9%
Chat	3.7%	Infostealer	7.6%	PUP:Generic.171138	10.0%
Computing and Internet	3.4%	Dropped:Trojan.Generic.6155725	7.4%	PUP:Generic.167772	5.2%
Search	2.3%	VBS/Generic	7.3%	Application.Generic.190952	4.9%
Peer-To-Peer	2.3%	Trojan:GIF/GIFrame.gen!A	7.0%	PUP:Generic.173909	4.8%
Games	1.9%	Dropped:Rootkit.49324	6.8%	PUP:Zwunzi!gen3	3.0%
Hosting Sites	1.7%	Infostealer.Gampass	6.0%	PUP:Agent.NFM	2.5%
News	1.7%	Dropped:Trojan.Generic.6137300	4.6%	PUP:Aurora	2.5%

July 2011

Endpoint Security Threats

The endpoint is often the last line of defense and analysis; however, the endpoint can often be the first-line of defense against attacks that spread using USB storage devices and insecure network connections. The threats found here can shed light on the wider nature of threats confronting businesses, especially from blended attacks and threats facing mobile workers. Attacks reaching the endpoint are likely to have already circumvented other layers of protection that may already be deployed, such as gateway filtering.

The table below shows the malware most frequently blocked targeting endpoint devices for the last month. This includes data from endpoint devices protected by Symantec technology around the world, including data from clients which may not be using other layers of protection, such as Symantec Web Security.cloud or Symantec Email AntiVirus.cloud.

Malware Name[4]	% Malware
W32.Ramnit!html	9.60%
W32.Sality.AE	8.83%
Trojan.Bamital	8.33%
W32.Ramnit.B!inf	7.43%
W32.Downadup.B	3.65%
W32.Almanahe.B!inf	2.68%
W32.Virut.CF	2.68%
W32.SillyFDC	2.06%
Trojan.ADH	1.80%
W32.Mabezat.B	1.78%

The most frequently blocked malware for the last month was W32.Ramnit!html. This is a generic detection for .HTML files infected by W32.Ramnit[5], a worm that spreads through removable drives and by infecting executable files. The worm spreads by encrypting and then appending itself to files with .DLL, .EXE and .HTM extensions. Variants of the Ramnit worm accounted for 17.3 percent of all malicious software blocked by endpoint protection technology in July.

For much of 2010, W32.Sality.AE had been the most prevalent malicious threat blocked at the endpoint; however, since June it has remained the second most prevalent malware blocked at the endpoint.

[4] *For further information on these threats, please visit: http://www.symantec.com/business/security_response/landing/threats.jsp*

[5] *http://www.symantec.com/security_response/writeup.jsp?docid=2010-011922-2056-99&tabid=2*

Many new viruses and Trojans are based on earlier versions, where code has been copied or altered to create a new strain, or variant. Often these variants are created using toolkits and hundreds of thousands of variants can be created from the same piece of malware. This has become a popular tactic to evade signature-based detection, as each variant would traditionally need its own signature to be correctly identified and blocked.

By deploying techniques, such as heuristic analysis and generic detection, it's possible to correctly identify and block several variants of the same malware families, as well as identify new forms of malicious code that seek to exploit certain vulnerabilities that can be identified generically. Approximately 17.7 percent of the most frequently blocked malware last month was identified and blocked using generic detection.

Best Practice Guidelines for Enterprises

1. **Employ defense-in-depth strategies**: Emphasize multiple, overlapping, and mutually supportive defensive systems to guard against single-point failures in any specific technology or protection method. This should include the deployment of regularly updated firewalls, as well as gateway antivirus, intrusion detection, intrusion protection systems, and Web security gateway solutions throughout the network.

2. **Monitor for network threat, vulnerabilities and brand abuse.** Monitor for network intrusions, propagation attempts and other suspicious traffic patterns, identify attempted connections to known malicious or suspicious hosts. Receive alerts for new vulnerabilities and threats across vendor platforms for proactive remediation. Track brand abuse via domain alerting and fictitious site reporting.

3. **Antivirus on endpoints is not enough:** On endpoints, signature-based antivirus alone is not enough to protect against today's threats and Web-based attack toolkits. Deploy and use a comprehensive endpoint security product that includes additional layers of protection including:

   - Endpoint intrusion prevention that protects against un-patched vulnerabilities from being exploited, protects against social engineering attacks and stops malware from reaching endpoints;
   - Browser protection for protection against obfuscated Web-based attacks;
   - Consider cloud-based malware prevention to provide proactive protection against unknown threats;
   - File and Web-based reputation solutions that provide a risk-and-reputation rating of any application and Web site to prevent rapidly mutating and polymorphic malware;
   - Behavioral prevention capabilities that look at the behavior of applications and malware and prevent malware;
   - Application control settings that can prevent applications and browser plug-ins from downloading unauthorized malicious content;
   - Device control settings that prevent and limit the types of USB devices to be used.

4. **Use encryption to protect sensitive data:** Implement and enforce a security policy whereby sensitive data is encrypted. Access to sensitive information should be restricted. This should include a Data Loss Protection (DLP) solution, which is a system to identify, monitor, and protect data. This not only serves to prevent data breaches, but can also help mitigate the damage of potential data leaks from within an organization.

5. **Use Data Loss Prevention to help prevent data breaches:** Implement a DLP solution that can discover where sensitive data resides, monitor its use and protect it from loss. Data loss prevention should be implemented to monitor the flow of data as it leaves the organization over the network and monitor copying sensitive data to external devices or Web sites. DLP should be configured to identify and block suspicious copying or downloading of sensitive data. DLP should also be used to identify confidential or sensitive data assets on network file systems and PCs so that appropriate data protection measures like encryption can be used to reduce the risk of loss.

6. **Implement a removable media policy**. Where practical, restrict unauthorized devices such as external portable hard-drives and other removable media. Such devices can both introduce malware as well as facilitate intellectual property breaches—intentional or unintentional. If external media devices are permitted, automatically scan them for viruses upon connection to the network and use a DLP solution to monitor and restrict copying confidential data to unencrypted external storage devices.

7. **Update your security countermeasures frequently and rapidly:** With more than 286M variants of malware detected by Symantec in 2010, enterprises should be updating security virus and intrusion prevention definitions at least daily, if not multiple times a day.

8. **Be aggressive on your updating and patching:** Update, patch and migrate from outdated and insecure browsers, applications and browser plug-ins to the latest available versions using the vendors' automatic update mechanisms. Most software vendors work diligently to patch exploited software vulnerabilities; however, such patches can only be effective if adopted in the field. Be wary of deploying standard corporate images containing older versions of browsers, applications, and browser plug-ins that are outdated and insecure. Wherever possible, automate patch deployments to maintain protection against vulnerabilities across the organization.

9. **Enforce an effective password policy**. Ensure passwords are strong; at least 8-10 characters long and include a mixture of letters and numbers. Encourage users to avoid re-using the same passwords on multiple Web sites and sharing of passwords with others should be forbidden. Passwords should be changed regularly, at least every 90 days. Avoid writing down passwords.

10. **Restrict email attachments:** Configure mail servers to block or remove email that contains file attachments that are commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF, and .SCR files. Enterprises should investigate policies for .PDFs that are allowed to be included as email attachments.

11. **Ensure that you have infection and incident response procedures in place:**
    - Ensure that you have your security vendors contact information, know who you will call, and what steps you will take if you have one or more infected systems;
    - Ensure that a backup-and-restore solution is in place in order to restore lost or compromised data in the event of successful attack or catastrophic data loss;
    - Make use of post-infection detection capabilities from Web gateway, endpoint security solutions and firewalls to identify infected systems;
    - Isolate infected computers to prevent the risk of further infection within the organization;
    - If network services are exploited by malicious code or some other threat, disable or block access to those services until a patch is applied;
    - Perform a forensic analysis on any infected computers and restore those using trusted media.

12. **Educate users on the changed threat landscape:**
    - Do not open attachments unless they are expected and come from a known and trusted source, and do not execute software that is downloaded from the Internet (if such actions are permitted) unless the download has been scanned for viruses;
    - Be cautious when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends;
    - Do not click on shortened URLs without previewing or expanding them first using available tools and plug-ins;
    - Recommend that users be cautious of information they provide on social networking solutions that could be used to target them in an attack or trick them to open malicious URLs or attachments;
    - Be suspicious of search engine results and only click through to trusted sources when conducting searches—especially on topics that are hot in the media;
    - Deploy Web browser URL reputation plug-in solutions that display the reputation of Web sites from searches;
    - Only download software (if allowed) from corporate shares or directly from the vendors Web site;
    - If users see a warning indicating that they are “infected” after clicking on a URL or using a search engine (fake antivirus infections), have users close or quit the browser using Alt-F4, CTRL+W or the task manager.

Best Practice Guidelines for Users and Consumers

1. **Protect yourself**: Use a modern Internet security solution that includes the following capabilities for maximum protection against malicious code and other threats:
   - Antivirus (file and heuristic based) and malware behavioral prevention can prevents unknown malicious threats from executing;
   - Bidirectional firewalls will block malware from exploiting potentially vulnerable applications and services running on your computer;
   - Intrusion prevention to protection against Web-attack toolkits, unpatched vulnerabilities, and social engineering attacks;
   - Browser protection to protect against obfuscated Web-based attacks;
   - Reputation-based tools that check the reputation and trust of a file and Web site before downloading; URL reputation and safety ratings for Web sites found through search engines.
2. **Keep up to date**: Keep virus definitions and security content updated at least daily if not hourly. By deploying the latest virus definitions, you can protect your computer against the latest viruses and malware known to be spreading in the wild. Update your operating system, Web browser, browser plug-ins, and applications to the latest updated versions using the automatic updating capability of your programs, if available. Running out-of-date versions can put you at risk from being exploited by Web-based attacks.
3. **Know what you are doing**: Be aware that malware or applications that try to trick you into thinking your computer is infected can be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware and shareware versions of software.
   - Downloading “free” “cracked” or “pirated” versions of software can also contain malware or include social engineering attacks that include programs that try to trick you into thinking your computer is infected and getting you to pay money to have it removed.
   - Be careful which Web sites you visit on the Web. While malware can still come from mainstream Web sites, it can easily come from less reputable sites sharing pornography, gambling and stolen software.
   - Read end-user license agreements (EULAs) carefully and understand all terms before agreeing to them as some security risks can be installed after an end user has accepted the EULA or because of that acceptance.
4. **Use an effective password policy:** Ensure that passwords are a mix of letters and numbers, and change them often. Passwords should not consist of words from the dictionary. Do not use the same password for multiple applications or Web sites. Use complex passwords (upper/lowercase and punctuation) or passphrases.
5. **Think before you click**: Never view, open, or execute any email attachment unless you expect it and trust the sender. Even from trusted users, be suspicious.
   - Be cautious when clicking on URLs in emails, social media programs even when coming from trusted sources and friends. Do not blindly click on shortened URLs without expanding them first using previews or plug-ins.
   - Do not click on links in social media applications with catchy titles or phrases even from friends. If you do click on the URL, you may end up “liking it” and sending it to all of your friends even by clicking anywhere on the page. Close or quit your browser instead.
   - Use a Web browser URL reputation solution that shows the reputation and safety rating of Web sites from searches. Be suspicious of search engine results; only click through to trusted sources when conducting searches, especially on topics that are hot in the media.
   - Be suspicious of warnings that pop-up asking you to install media players, document viewers and security updates; only download software directly from the vendor’s Web site.
6. **Guard your personal data**: Limit the amount of personal information you make publicly available on the Internet (including and especially social networks) as it may be harvested and used in malicious activities such as targeted attacks, phishing scams.
   - Never disclose any confidential personal or financial information unless and until you can confirm that any request for such information is legitimate.

- Review your bank, credit card, and credit information frequently for irregular activity. Avoid banking or shopping online from public computers (such as libraries, Internet cafes, etc.) or from unencrypted Wi-Fi connections.
- Use HTTPS when connecting via Wi-Fi networks to your email, social media and sharing Web sites. Check the settings and preferences of the applications and Web sites you are using.

About Symantec.cloud Intelligence

Symantec.cloud Intelligence is a respected source of data and analysis for messaging security issues, trends and statistics. Symantec.cloud Intelligence publishes a range of information on global security threats based on live data feeds from more than 15 data centers around the world scanning billions of messages and Web pages each week. Team Skeptic™ comprises many world-renowned malware and spam experts, who have a global view of threats across multiple communication protocols drawn from the billions of Web pages, email and IM messages they monitor each day on behalf of 31,000 clients in more than 100 countries. More information is available at www.messagelabs.com/intelligence.

About Symantec

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

NO WARRANTY. The information contained in this report is being delivered to you AS-IS, and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the information contained herein is at the risk of the user. This report may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice. No part of this publication may be copied without the express written permission of Symantec Corporation, 350 Ellis Street, Mountain View, CA 94043.