MessageLabs
Now part of Symantec

MessageLabs Intelligence: Juni und zweites Quartal 2009

Cutwails schnelle Auferstehung und die wachsende Gefahr, sich per Instant Messaging auch Instant Malware einzufangen

Herzlich willkommen zur aktuellen Ausgabe des Monatsberichts von MessageLabs Intelligence für Juni und das zweite Quartal. Dieser Report informiert Sie über aktuelle Gefahrentrends im Juni 2009 und hält Sie über den kontinuierlichen Kampf gegen Viren, Spam und andere unwillkommene Online-Inhalte auf dem Laufenden.

Die wichtigsten Ergebnisse im Überblick

- *Spam: 90,4 Prozent im Juni (gegenüber dem Vormonat unverändert).*
- *Viren: Eine von 269,4 E-Mails enthielt im Juni ein Schadprogramm (eine Steigerung um 0,06 Prozentpunkte im Vergleich zum Mai).*
- *Phishing: Hinter einer von 280,4 E-Mails verbarg sich ein Phishing-Angriff (gegenüber dem Vormonat unverändert).*
- *Gefährliche Websites: Pro Tag wurden 1.919 neue Internetseiten gesperrt (eine Zunahme um 67,0 Prozent gegenüber Mai).*
- *Bei 58,8 Prozent der über das Surfen im Internet verbreiteten Malware handelte es sich im Juni um neue Angriffe (ein Plus von 24,6 Prozentpunkten im Vergleich zum Vormonat).*
- *Das Cutwail-Botnet meldet sich nach einem Rückschlag fast umgehend zurück.*
- *Die Macht der Botnets: 83,2 Prozent des Spam-Aufkommens entfielen im Juni auf diesen Verbreitungsweg.*
- *Angriffe mit Grafik-Spam setzten sich fort und zeichneten im Juni für 8 bis 10 Prozent der Spam-Belastung verantwortlich.*
- *Malware-Attacken über Instant-Messaging-Systeme auf dem Vormarsch: Jeder 78. Link in IM-Sofortnachrichten verweist auf gefährliche Websites.*
- *Der HITECH-Act verschärft den Handlungsdruck im Gesundheitssektor.*

Die Analyse der Ergebnisse

Cutwails schnelle Auferstehung: Eine Demonstration der Botnet-Stärke

Am Morgen des 5. Juni 2009 erlebte mit Cutwail eines der größten und aktivsten Botnets, die für den Versand von Spam verantwortlich sind, für mehrere Stunden eine erhebliche Störung. Ursache für den Ausfall war, dass die Federal Trade Commission der Vereinigten Staaten zuvor den in Kalifornien ansässigen (und auch unter 3FN und APS Telecom firmierenden) Internet Service Provider (ISP) Pricewert LLC vom Netz genommen hatte. Das Botnet Cutwail, das auch unter dem Namen Pandex bekannt ist, war erstmals im Januar 2007 mit der Verbreitung von Malware in Erscheinung getreten.

botnet	% of spam	spam/day	spam/min	spam/bot /min	estimated botnet size	top 3 countries of infection
Cutwail	45.8%	74,115,721,081	51,469,251	257	1400k - 2100k	Brazil (14%), RepKorea (14%), USA (10%)
Rustock	4.5%	7,231,588,803	5,021,937	97	640k - 960k	Brazil (12%), India (10%), Turkey (9%)
Grum	6.0%	9,624,703,890	6,683,822	76	600k - 900k	Russia (27%), Ukraine (11%), Brazil (8%)
Donbot	3.2%	5,150,182,696	3,576,516	62	360k - 540k	Brazil (12%), India (12%), Turkey (8%)
Bagle	1.7%	2,716,295,255	1,886,316	53	300k - 450k	Brazil (14%), USA (9%), Argentina (8%)
Xarvester	0.2%	285,121,953	198,001	41	30k - 50k	Poland (11%), Brazil (11%), Turkey (7%)
Mega-D	9.3%	15,043,613,046	10,446,954	560	460k - 700k	Brazil (17%), India (7%), Turkey (7%)
Gheg	1.4%	2,216,672,839	1,539,356	69	170k - 250k	Turkey (24%), Vietnam (17%), India (10%)
Asprox	0.2%	382,667,732	265,741	146	11k - 17k	Brazil (25%), Argentina (9%), Poland (8%)
Darkmailer	0.1%	93,954,453	65,246	590	1k	USA (22%), France (16%), RepKorea (11%)
Unclassified Botnets	10.5%	17,012,784,584	11,814,434	93	860k - 1300k	Brazil (14%), USA (6%), India (5%)

Abbildung 1: Übersicht über die aktiven Botnets (Stand: Juni 2009)

Zu seiner besten Zeit war Cutwail mit 1,5 bis 2 Millionen aktiven, auf manipulierte Computer geschmuggelten Software-Bots das vielleicht größte Botnet aller Zeiten. Vor der Abschaltung des ISPs McColo im November 2008 wurde es mit geschätzten 25 Prozent des gesamten Spam-Aufkommens in Verbindung gebracht. Im Mai 2009 zeichnete Cutwail sogar für 35 Prozent aller Spam-Mails verantwortlich. Zu den größeren Spam-Wellen, die Cutwail lanciert hat, gehört auch die Kampagne für die Diätpille „Acai Berry“, über die MessageLabs Intelligence im Mai berichtet hat.

Als dieser Monatsbericht verfasst wurde, war der aktuelle Stand, dass sich Cutwail nach dem Rückschlag bereits wieder auf ein Drittel seiner originalen Kapazität erholt hatte. Zwar litt Cutwail noch unter der jüngsten ISP-Abschaltung, zeigte sich aber nicht so schlimm betroffen wie das rivalisierende Botnet Srizbi, das nach der Schließung von McColo im November des Vorjahres völlig am Boden lag. Die Tatsache, dass sich Cutwail binnen weniger Stunden regenerieren konnte, unterstreicht, welche Fortschritte die Spam-Szene seit der Abschaltung von McColo gemacht hat. Spammer haben mittlerweile fraglos gelernt, wie wichtig es für ihre Zwecke ist, dass sie über ein Backup für ihre Command-and-Control-Server verfügen.

Hintergrund der Schließung von Pricewert LLC war, dass dieser ISP unter Verdacht steht, an der Bereitstellung von Botnets sowie der Verbreitung von verbotenen, gefährlichen und schädlichen Inhalten wie zum Beispiel Spam oder Kinderpornografie beteiligt gewesen ist.

Cutwail	Zweifellos das mächtigste aller Botnets. Konnte seit März sowohl seine Größe als auch den Durchsatz pro Bot verdoppeln.
Rustock	Sorgt immer noch mit explosionsartig intensiviertem Spam-Versand für Aufsehen und offenbart in diesen Zeiträumen sein wahres Potenzial zur Verbreitung solcher Inhalte. Durchläuft aber auch regelmäßig Phasen ohne jedwede Aktivität.
Grum	Weiterhin sehr unregelmäßig aktiv, was den Ausstoß betrifft. Hat aber in den vergangenen Monaten an Aktivität zugelegt.
Donbot	Eines der wichtigsten Botnets, aber zuletzt weniger aktiv als in der Vergangenheit.
Bagle	Kleiner als die wirklich großen Botnets, beweist aber Beständigkeit beim Versand fragwürdiger Inhalte und dehnt sich noch weiter aus.
Xarvester	Anfang des Jahres noch eines der dominanten Botnets. Hat in den letzten Monaten aber drastisch in Bezug auf seine Größe und Aktivität eingebüßt.
Mega-D	Zu Beginn des Jahres noch das bedeutendste Botnet. Hat seither jedoch kontinuierlich an Größe verloren. Hinsichtlich des Spam-Versands pro Bot und Minute noch immer eines der umtriebigsten Botnets.
Gheg	Ein kleineres Botnet mit jedoch konstantem Ausstoß.
Asprox	Uneinheitlich, was den Ausstoß betrifft. Hat jedoch zuletzt angefangen, die infizierten Rechner stärker zu beanspruchen, um den Durchsatz pro Bot zu steigern.
Darkmailer	Ein sehr kleines Botnet, das jedoch einfach durch die enorme Zahl an pro Bot und Minute verschickten Spam-Mails in den Blickpunkt geraten ist.

Eine Charakterisierung der zehn Botnets, die im Juni 2009 die größte Aktivität gezeigt haben.

Im Juni 2009 entfielen insgesamt 83,2 Prozent des Spam-Aufkommens auf Botnets. Der verbleibende Rest wurde über manipulierte E-Mail-Server und über Nutzerkonten bei Webmail-Diensten verschickt. Einige der kleineren Botnets sind mittlerweile in der Lage, den Versand von Spam-Inhalten über Webmail-Accounts so zu steuern, dass es den Anschein hat, als würde hinter jeder dieser Absender-Adressen eine reale Person stehen.

Wie MessageLabs Intelligence bereits in früheren Monatsberichten erläutert hat, werden viele dieser Webmail-Accounts massenweise in automatischer Manier generiert. Dazu kommen spezielle Tools zur Aushebelung von CAPTCHA-Prüfungen zum Einsatz, mit denen sich die Rätsel in Form von zu entschlüsselnden Bildern und Audio-Dateien umgehen lassen, an deren Lösung viele Websites die Nutzeranmeldung oder -registrierung knüpfen. Als alternative Herangehensweise lassen sich auch die Dienste von Firmen in Anspruch nehmen, die sich darauf spezialisiert haben, CAPTCHAs mit Hilfe von im 24-Stunden-Betrieb eingesetzten Hilfskräften manuell zu lösen. Angeboten werden solche Jobs häufig als EDV-Tätigkeit. Wer sich darauf einlässt, darf jedoch lediglich mit einem Verdienst von zwei bis drei US-Dollar pro 1.000 erstellten Nutzerkonten rechnen, für die Spammern dann anschließend 30 bis 40 US-Dollar in Rechnung gestellt werden.

Grafik-Spam weiter auf dem Vormarsch

Spam in Form von Bilddateien, der für den signifikanten Anstieg der Spam-Belastung im Mai verantwortlich gemacht wurde, ist im Juni weiterhin mit Nachdruck zum Einsatz gekommen und war nun für 8 bis 10 Prozent aller Spam-Mails verantwortlich. Dabei hängen die Urheber diese Grafiken ihren E-Mails vornehmlich direkt als Attachments an, anstatt Bilddateien irgendwo ins Netz zu stellen und per HTML-Code in ihre Nachrichten einzubetten. Einige der zuletzt verbreiteten Spam-Bilder enthielten zur Verschleierung auch automatisch generierte Hintergrundmuster.

Abbildung 2: Grafik-Spam mit zur Verschleierung eingesetzten Hintergrundmustern.

Grafik-Spam wird beinahe ausnahmslos über Botnets verbreitet, wobei die verschickten Nachrichten oft keinerlei Links enthalten. Stattdessen finden sich die Namen der beworbenen Spam-Seiten häufig in den Bildern selbst.

Wachsende Virengefahr beim Instant Messaging

Ende 2008 hatten die Erhebungen von MessageLabs Intelligence ergeben, dass jeder 200. Link (0,50 Prozent), der über öffentliche IM-Systeme (Instant Messaging) verschickt wurde, eine Malware-Gefahr darstellte. Das heißt, die betreffenden Websites enthielten Schadprogramme, die Sicherheitslücken anfälliger Web-Browser oder Browser-Plug-ins ausnutzten, um sich mittels Drive-by-Attacken unbemerkt von Besuchern auf deren Rechnern einzunisten. Im Juni hat MessageLabs Intelligence nun eine Vergleichsstudie unternommen, die offenbart, dass sich diese Art von Bedrohung mittlerweile verschärft hat. Die aktuellen Analysen ergaben, dass heute jede 405. über IM-Kanäle verschickte Nachricht (0,25 Prozent) einen Link enthält (ohne Berücksichtigung von Haftungsausschlusserklärungen und Hinweisen auf andere gesetzliche Bestimmungen, die für bestimmte Organisationen angeraten sind) und dass von diesen Links wiederum jeder 78. auf eine Website mit Malware-Inhalten verweist. Das ist ein Anteil von 1,28 Prozent und bedeutet eine Zunahme deratiger Angriffe um 0,78 Prozentpunkte. Vor dem Hintergrund dieser Zahlen geht MessageLabs Intelligence davon aus, dass jeder 80. IM-Anwender einmal im Monat über diesen Kommunikationskanal eine Sofortnachricht mit einem gefährlichen Link erhält.

IT-Investitionen im Gesundheitswesen

Am 17. August 2009 läuft in den USA die im so genannten HITECH-Act (Health Information Technology for Economic and Clinical Health) gesetzte Frist ab. Bis dahin stehen das dortige Gesundheitsministerium (United States Department of Health and Human Services) und die Federal Trade Commission (FTC) in der Pflicht, ihre Regelungen zu vereinheitlichen und endgültige Übergangsbestimmungen zu verabschieden. Der HITECH-Act wurde als Teil des US-Konjunkturprogramms 2009 (American Recovery and Reinvestment Act) erlassen und benennt Auflagen im Hinblick auf die Bekanntmachung etwaiger Datenschutzverletzungen bei geschützten Gesundheitsinformationen (Protected Health Informations − PHI).

Angesicht der Regierungsgelder in Millionenhöhe, die derzeit in die Digitalisierung und den Schutz von Patientendaten fließen, sind die Überschneidungen zwischen Medizin und Informationstechnologie heute größer denn je. Organisationen aus allen Teilen des Gesundheitssektors stehen völlig zu Recht spürbar unter Druck, gesetzliche Vorgaben wie den HITECH-Act umzusetzen.

Die Analysen von MessageLabs Intelligence decken auf, dass es für die Akteure des Gesundheitssektors eine steigende Notwendigkeit gibt, sich gegen Online-Gefahren zu wappnen. Die folgenden Kurvendiagramme zeigen, dass die Spam-Belastung in der Healthcare-Industrie in den vergangenen Monaten zugenommen hat und noch vor Ende des Jahres 2009 die 90-Prozent-Marke übersteigen könnte. Weiterhin hat sich auch die Zahl der gegen Organisationen der Gesundheitsbranche gerichteten, via E-Mail verbreiteten Schadprogramm-Angriffe seit Anfang 2009 mehr als verdoppelt.

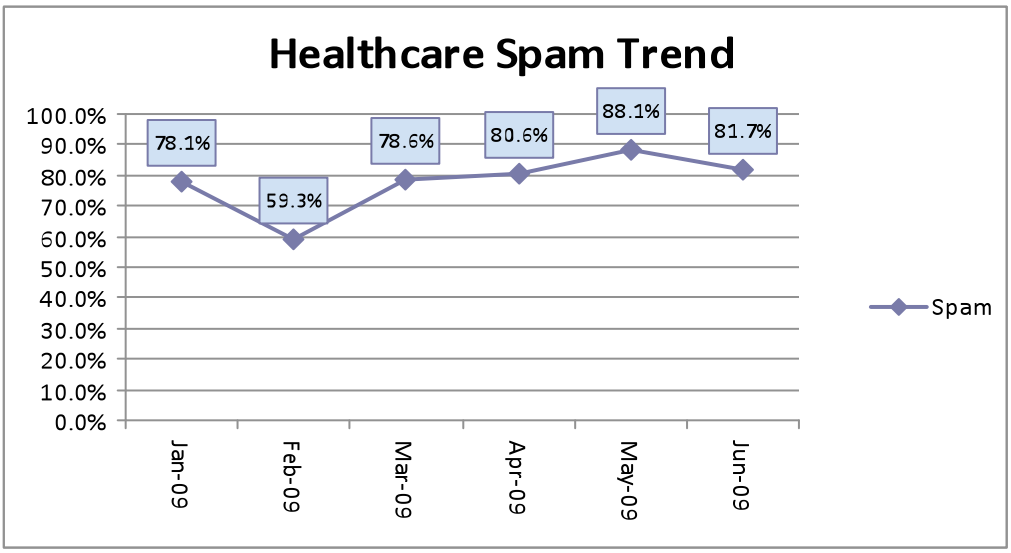


Abbildung 3: Entwicklung der Spam-Belastung im Gesundheitsektor

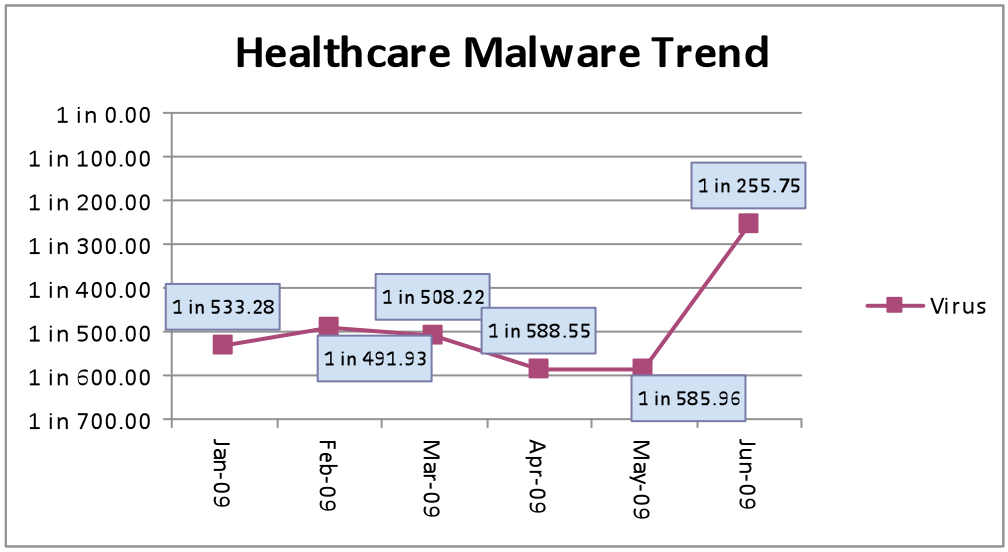
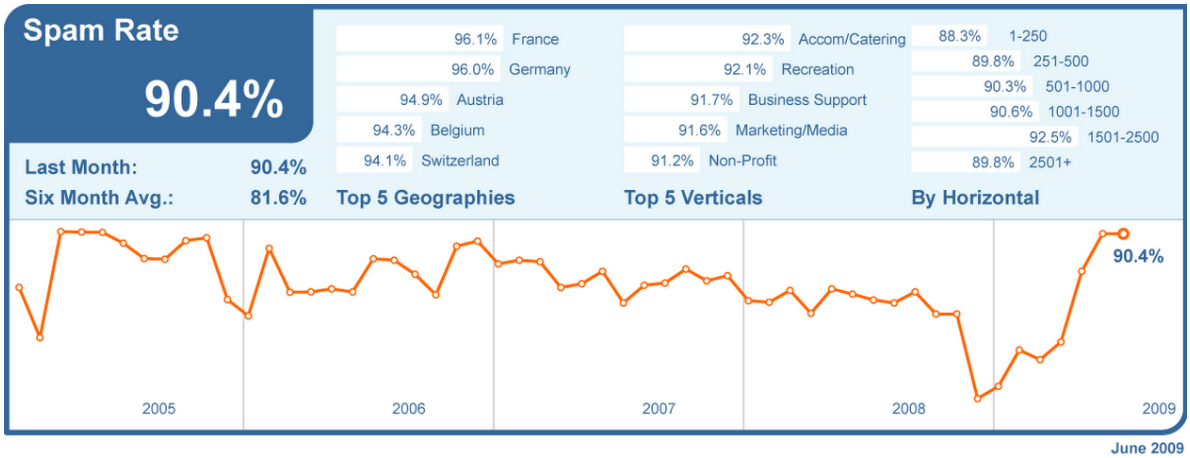


Abbildung 4: Entwicklung der Malware-Belastung im Gesundheitsektor

Globale Trend- und Content-Analyse

Die Anti-Spam- und Anti-Viren-Dienste von MessageLabs konzentrieren sich auf die Identifikation und Abwehr unerwünschter Online-Nachrichten, die aus unbekannten zweifelhaften Quellen stammen und an gültige E-Mail-Adressen gerichtet sind.

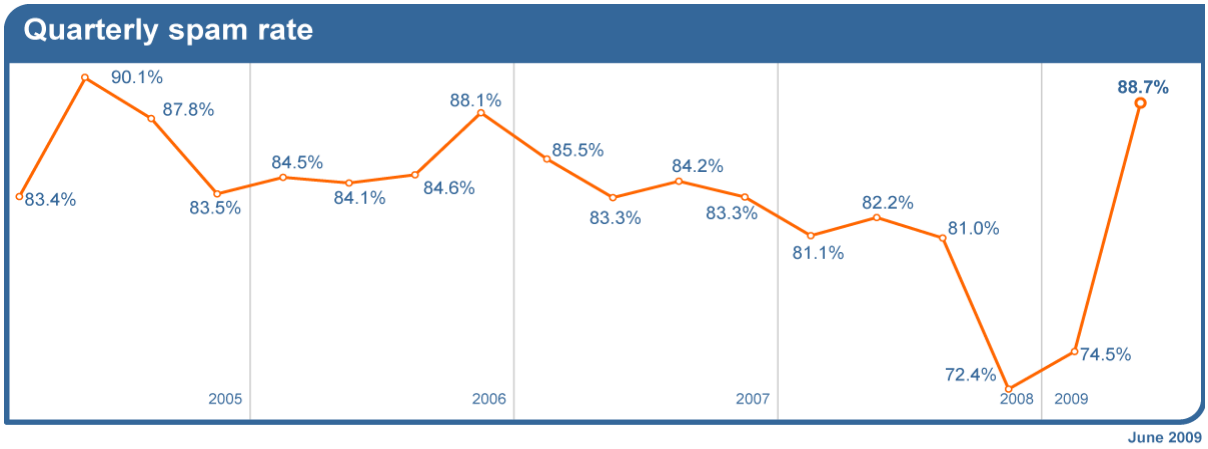
Spam-Schutz mit Skeptic™: Im Juni 2009 belief sich der weltweite Anteil von Spam-Nachrichten am E-Mail-Verkehr aus neuen oder bisher nicht als bösartig bekannten Quellen auf 90,4 Prozent (oder eine von 1,1 E-Mails) und erreichte damit exakt das Niveau des Vormonats.



Ein Anstieg der Spam-Quote um 8,6 Prozentpunkte auf 96,1 Prozent machte Frankreich im Juni zu dem Land, das weltweit am meisten unter Spam zu leiden hatte. Während die Spam-Quote in den USA auf 78,4 Prozent zurückging und auch in Kanada auf 72,2 Prozent sank, legte sie in Großbritannien auf 90,3 Prozent zu. In Deutschland erreichte die Spam-Quote einen Wert von 96,0 Prozent und in den Niederlanden von 93,9 Prozent. In Australien entfielen 88,8 Prozent des E-Mail-Verkehrs auf Spam und in Japan 67,1 Prozent.

Mit einer Spam-Quote von 92,3 Prozent stand das Hotel- und Gaststättengewerbe im Juni stärker unter Beschuss von Spam-Mails als jede andere Branche. Der Bildungssektor erreichte eine Spam-Quote von 90,3 Prozent und die Chemie- und Pharma-Industrie von 88,6 Prozent. Im Einzelhandel belief sich dieser Wert auf 90,2 Prozent, bei Behörden auf 90,8 Prozent und in der Finanzindustrie auf 87,5 Prozent.

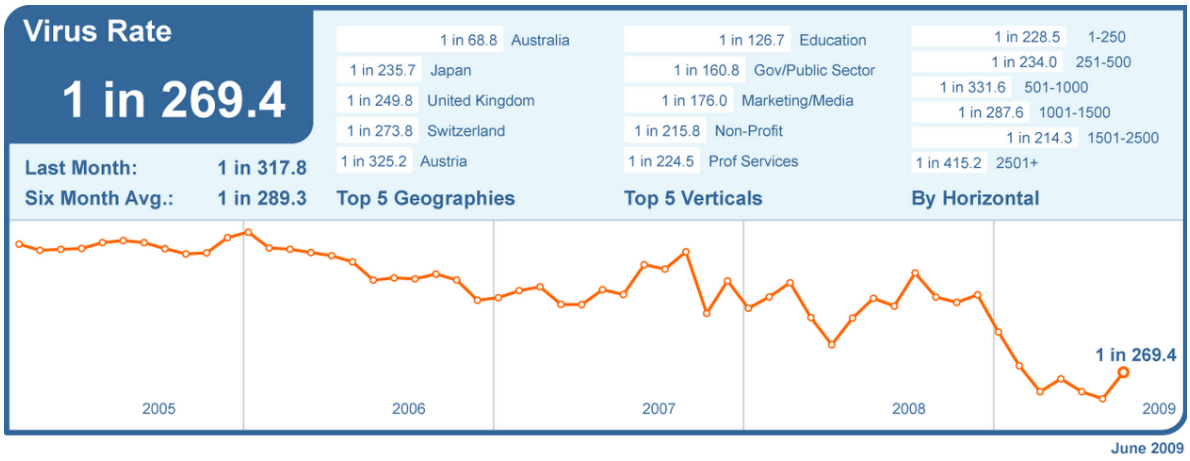
Quartalsanalyse: Wie dem folgenden Kurvendiagramm zu entnehmen ist, betrug die Spam-Quote im zweiten Quartal 2009 durchschnittlich 88,7 Prozent, nachdem sie in den ersten drei Monaten noch bei 74,5 Prozent gelegen hatte.



Viren- und Trojaner-Abwehr mit Skeptic™: Der weltweite Anteil von per E-Mail verbreiteten Viren am gesamten E-Mail-Verkehr, der von neuen oder bis dato nicht als schädlich bekannten Absendern stammte, belief sich im Juni auf 1 zu 269,4 (bzw. 0,37 Prozent). Das bedeutet ein Plus von 0,06 Prozentpunkten gegenüber dem Vormonat.

Zurückzuführen war der leichte Anstieg der Viren-Belastung zum Teil auf eine Welle von via E-Mail lancierten Malware-Attacken. Die zu diesem Zweck verschickten Nachrichten machten den Eindruck, als würden sie von bekannten und angesehenen international tätigen Transportunternehmen stammen, und informierten die Empfänger, dass diesen ein angebliches Paket nicht hätte zugestellt werden können. Dies sollte die Adressaten dazu verleiten, ein Schadprogramm im Anhang zu öffnen, das als Rechnung für das nicht existierende Paket getarnt war.

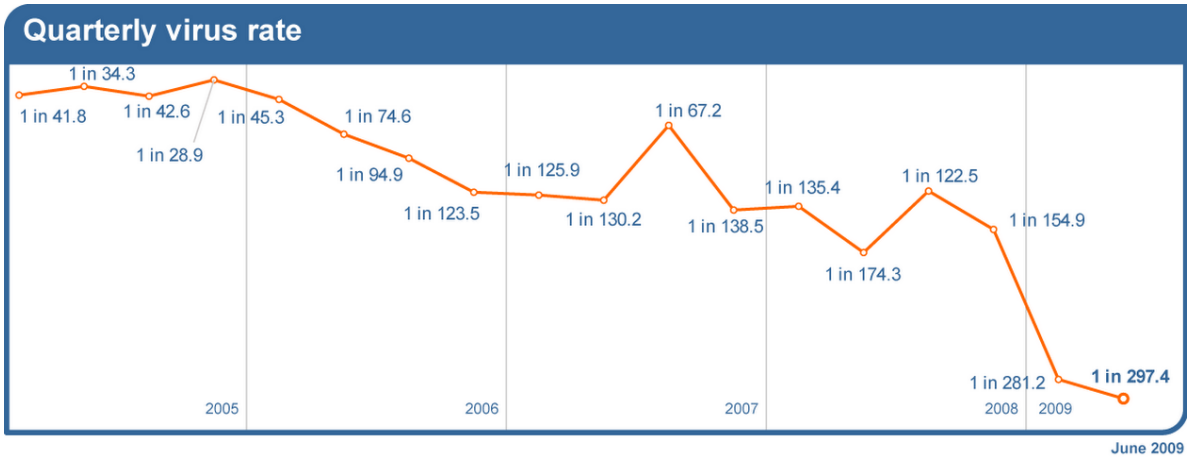
Ein Anteil von 10,4 Prozent der via E-Mail verbreiteten Malware beruhte im Juni auf Links zu gefährlichen Websites. Das sind 3,4 Prozentpunkte mehr als noch im Mai. Als vermeintliche Online-Postkarten getarnte Mails waren im Juni für 66,5 Prozent dieser gefährlichen Links verantwortlich.



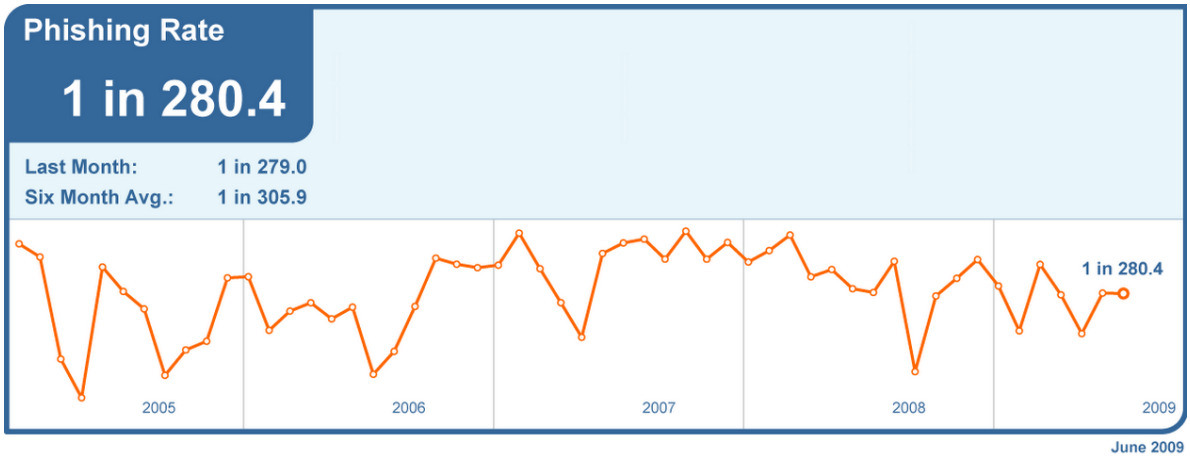
In Australien stieg der Anteil schadprogrammverseuchter E-Mails im Juni um 1,29 Prozentpunkte auf 1 zu 68,8. Mit dieser Quote übernahm das Land den ersten Platz im weltweiten Viren-Ranking. In den Vereinigten Staaten betrug der Anteil virenbelasteter E-Mails 1 zu 371,7, und in Kanada 1 zu 423,7. In Deutschland belief sich das entsprechende Verhältnis auf 1 zu 444,0 und in den Niederlanden auf 1 zu 644,5. Für Hongkong konnte MessageLabs Intelligence eine Viren-Quote von 1 zu 354,7 ermitteln und für Japan von 1 zu 235,7.

Trotz eines Rückgangs der Viren-Quote um 0,10 Prozentpunkte auf einen Anteil von 1 zu 126,7 verteidigte der Bildungssektor seinen ersten Platz im Ranking der Branchen, die sich mit dem höchsten Anteil an verseuchten E-Mails konfrontiert sahen. Bei IT-Dienstleistern belief sich die Viren-Quote auf 1 zu 358,0, bei Einzelhandelsunternehmen auf 1 zu 493,6 und bei Finanzdienstleistern auf 1 zu 259,1.

Quartalsanalyse: Das folgende Kurvendiagramm veranschaulicht, dass sich für das zweite Quartal 2009 eine Viren-Quote von durchschnittlich 1 zu 297,4 ergab, während für das erste Quartal des Jahres ein Vergleichswert von 1 zu 281,2 gemessen wurde.

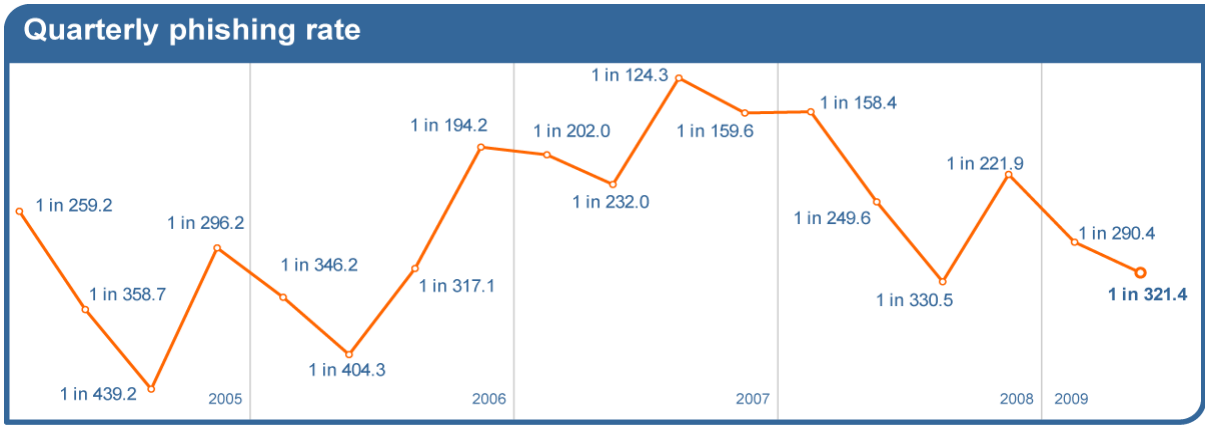


Phishing: Im Juni ist die Phishing-Quote im Vergleich zum Mai weitgehend unverändert geblieben. Bei einer von 280,4 E-Mails (bzw. 0,36 Prozent) handelte es sich um einen Versuch zum Auskundschaften von Authentisierungsdaten. Betrachtet in Relation zu allen abgefangenen, per E-Mail verbreiteten Malware-Angriffen beispielsweise in Form von Viren und Trojanern betrug der Anteil von Phishing-Nachrichten im Juni 96,1 Prozent. Das sind 6,4 Prozentpunkte mehr als noch im Mai.



Die Phishing-Angriffe erfolgen weiterhin in Wellen, wobei sie sich jeweils auf Finanzinstitute in bestimmten Ländern konzentrieren, bevor sich die Attacken dann wieder auf andere Ziele verlagern. Festzustellen ist zudem, dass ein zunehmender Anteil der Phishing-Aktivitäten in Zusammenhang mit der Verfügbarkeit von „Selbstbaukästen“ für derartige Zwecke steht. Ebenso auf dem Vormarsch ist die Manipulation eigentlich vertrauenswürdiger Websites, um auf diesem Wege Phishing-Seiten ins Netz zu stellen.

Quartalsanalyse: Das nachstehende Kurvendiagramm zeigt, dass für das zweite Quartal 2009 eine Phishing-Quote von 1 zu 321,4 ermittelt wurde, nachdem diese sich im ersten Quartal des Jahres auf 1 zu 290,4 belaufen hatte.



Skeptic™ Web Security Services Version 2.0: Die Website-Kategorie „Werbung & Popups“ war im Juni mit einem Anteil von 61,6 Prozent der häufigste Auslöser von regel- und richtliniengesteuerten Filterungsaktivitäten, die im Rahmen des Dienstes MessageLabs Web Security für Geschäftskunden erfolgt sind. Gegenüber Mai bedeutet dies eine Zunahme um 0,2 Prozentpunkte.

Die Analyse der von diesem Dienst zur Web-Sicherheit getroffenen Maßnahmen zeigt, dass es sich im Juni bei 58,8 Prozent aller abgefangenen, über das Internet verbreiteten Schadprogramme um neue Angriffe gehandelt hat. Im Vormonat war dieser Anteil noch um 24.6 Prozent geringer ausgefallen. Durchschnittlich hat MessageLabs Intelligence im Juni pro Tag 1.919 neue Seiten aufgespürt, auf denen Malware und andere möglicherweise unerwünschte Programme wie etwa Spy- und Adware hinterlegt waren. Das waren 67,0 Prozent mehr als noch im Mai.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	61.6%	Infostealer.Gampass	23.4%	PUP:WebToolbar.Win32.MyWebSea...	60.9%
Streaming Media	11.1%	Generic Dropper.eb	8.4%	PUP:SAHAgent	7.9%
Downloads	4.5%	Trojan-Downloader.JS.Gumblar.a	4.4%	PUP:WebToolbar.Win32.Zango.ca	4.0%
Games	3.7%	Trojan.Fakeavalert	3.7%	PUP:RemoteAdmin.Win32.WinVNC.1102	3.6%
Blogs & Forums	2.5%	Trojan Horse	2.6%	PUP:PSWTool.Win32.WinPassViewer.q	2.2%
Chat	2.0%	Trojan.JS.Agent.xz	2.3%	PUP:WebToolbar.Win32.Zango.cb	2.0%
Adult/Sexually Explicit	1.8%	Obfuscated Script.f	2.1%	PUP:NetTool.Win32.Portscan.c	1.8%
Peer-to-Peer	1.5%	Bloodhound.DirActCOM	2.1%	PUP:RemoteAdmin.Win32.WinVNC.c	1.0%
Computing & Internet	1.3%	Trojan.JS.Agent.ahc	1.7%	PUP:PSWTool.Win32.Messen.ct	1.0%
Personals & Dating	1.3%	Trojan-Downloader.JS.Iframe.aqu	1.6%	PUP:AdTool.Win32.MyWebSearch.br	1.0%

June 2009

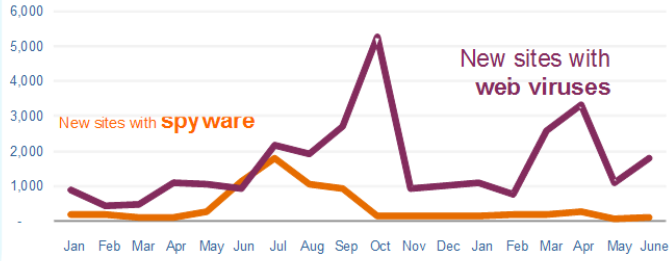
Auf die Gefahrenklasse „Nicht klassifiziert“, für die alle neuen und bisher noch nicht eingestuften Websites herangezogen werden, entfielen im Juni 0,6 Prozent der unterbundenen Website-Zugriffe. Dabei kann es sich um Seiten, die für betrügerische und anrüchige Zwecke wie beispielsweise Phishing und Spam verwendet werden, ebenso handeln wie um gerade erst von Firmen mit tadellosem Leumund eingerichtete Web-Auftritte und Domains, die bis dato einfach noch nicht kategorisiert wurden. Durch Rückgriff auf den MessageLabs-Service zur Web-Sicherheit machen sich Kunden im Umgang mit solchen Seiten einen flexiblen Ansatz zunutze: Alle von solchen Websites heruntergeladenen Inhalte werden mit einer einzigartigen Kombination aus Skeptic-Technologien und kommerziellen Virenscannern auf Schadprogramme hin untersucht. So können Kunden ihre Online-Sicherheit wahren, ohne dass es erforderlich wäre, derartige Seiten vorsichtshalber komplett zu sperren.

Das folgende Kurvendiagramm veranschaulicht, wie im Laufe des Monats Mai das Aufkommen an täglich neu zu sperrenden Viren- und Trojaner-Seiten gestiegen ist und wie sich im Vergleich dazu die entsprechende Zahl der pro Tag blockierten Websites mit Spy- und Adware entwickelt hat.

Web Security Services (Version 2.0) Activity:

New Malware Sites per Day

New sites with **spyware**	123/day
New sites with **web viruses**	1,796/day
Total	**1,919/day**

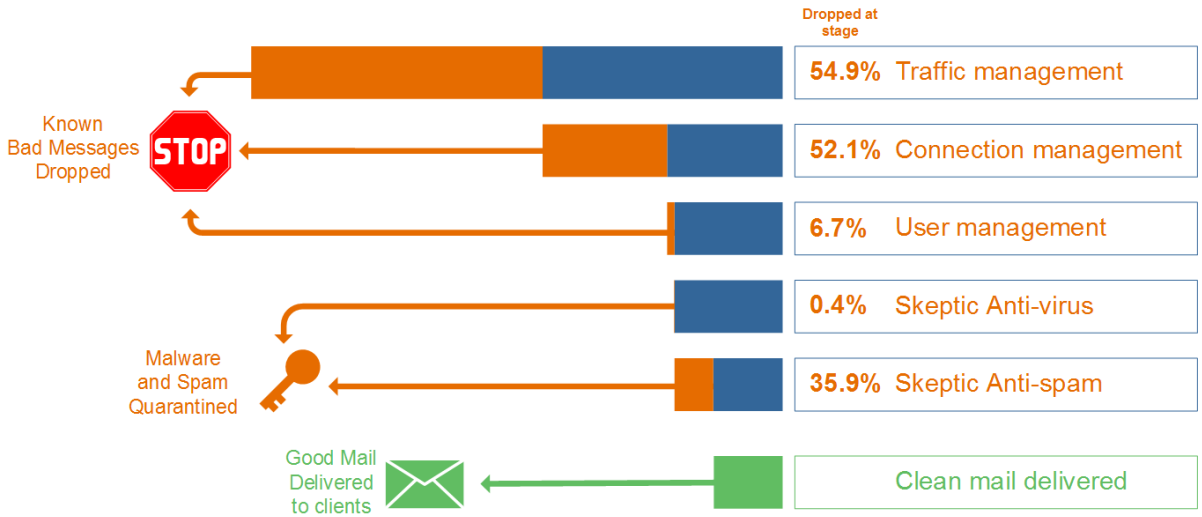


June 2009

Traffic-Management

Mittels Traffic-Management gelingt es weiterhin, die Gesamtmenge der übermittelten Nachrichten durch Techniken zu senken, die auf Protokoll-Ebene aktiv sind. Dabei werden unerwünschte Absender identifiziert und die entsprechenden Mail-Server-Verbindungen über Funktionen, die in das TCP-Protokoll eingebettet sind, gezielt verlangsamt. Auf diese Weise werden bekannte Spam-Formen auf der Eingangsseite erheblich ausgebremst, während die reibungslose Übermittlung aller zulässigen E-Mails gewährleistet bleibt.

Im Juni wurden im Rahmen der MessageLabs-Dienste durchschnittlich 6,44 Milliarden SMTP-Verbindungen pro Tag verarbeitet. Davon wurden 54,9 Prozent im Zuge des Traffic-Managements gedrosselt, weil es sich um eindeutig schädlichen und unerwünschten E-Mail-Verkehr handelte. Der Rest der Verbindungen hatte anschließend die Prüftechnologien von MessageLabs Connection-Management und MessageLabs Skeptic™ zu durchlaufen.



Connection-Management
Das Connection-Management erweist sich als ein sehr effektives Instrument, um insbesondere eine Adressbücher-Plünderung, Brute-Force-Attacken und E-Mail-basierende Denial-of-Service-Angriffe zu stoppen – also solche Techniken, bei denen unerwünschte Massenmails ein Unternehmen überfluten und auf diese Weise dessen Geschäftskommunikation stören sollen. Aktiv ist das Connection-Management auf SMTP-Ebene, und es verwendet dabei Verfahren zur *SMTP-Validierung*, um zu überprüfen, inwieweit aufzubauende Mail-Server-Verbindungen tatsächlich legitim sind. Dabei ist es möglich, unerwünschte E-Mails von Urhebern zu erkennen, die bereits für den Versand von Spam und Viren bekannt sind. Solche Quellen werden eindeutig als offene Proxy-Speicher oder als Botnets identifiziert, und die Verbindungsabfrage wird entsprechend zurückgewiesen. Im Juni wurden auf diese Weise durchschnittlich 52,1 Prozent aller eingehenden Mails abgefangen, da diese von Botnets oder aus anderen bekannten Schadprogramm-Quellen stammten, und infolgedessen aussortiert.

User-Management
Eine *Adress-Prüfung der registrierten Anwender* senkt die Gesamtmenge an E-Mails, die an eingetragene Domains übermittelt werden. Denn das Verfahren verwirft alle Verbindungen, die an ungültige oder nicht existierende Einzelempfänger gerichtet sind. Im Juni wurden durchschnittlich 6,7 Prozent der eingehenden Mails wegen ungültiger Adressen abgefangen. Dahinter verbargen sich versuchte Directory-Attacken auf Domains, die somit verhütet werden konnten.

Über MessageLabs Intelligence
MessageLabs Intelligence ist ein angesehener Anbieter von Daten und Analysen zu Themen, Trends und Statistiken rund um die Sicherheit von Internet-, E-Mail- und Instant-Messaging-Anwendungen. Mit Hilfe von 14 Rechenzentren in aller Welt, die pro Woche mehrere Milliarden Mails überprüfen, erfasst MessageLabs Intelligence fortwährend Live-Daten und veröffentlicht auf dieser Grundlage vielfältige Informationen zur aktuellen globalen Bedrohungssituation. Zum MessageLabs Team Skeptic™ gehören zahlreiche weltweit anerkannte Malware- und Spam-Experten, die über die Grenzen einzelner Kommunikationskanäle hinweg ein umfassendes Verständnis der Online-Gefahren mitbringen. Diese besondere Expertise stützt sich auf exakte Daten zu den Milliarden von Websites, E-Mails und IM-Nachrichten, die sie tagtäglich im Auftrag von 19.000 Kunden aus 86 Ländern überprüfen. Weiterführende Informationen finden sich im Internet unter www.messagelabs.com/intelligence.

Über Symantec
Symantec ist ein weltweit führender Anbieter von Infrastuktur-Software, mit der sich Unternehmen und Privatpersonen sicher und vertrauensvoll in einer vernetzen Welt bewegen können. Das Unternehmen unterstützt Kunden beim Schutz ihrer Infrastrukturen, Informationen und Interaktionen durch Software und Dienstleistungen, die Risiken der IT-Sicherheit, Verfügbarkeit, Compliance und Leistungsfähigkeit adressieren. Symantec hat seinen Hauptsitz in Cupertino, Kalifornien und betreibt Niederlassungen in mehr als 40 Ländern. Mehr Informationen unter www.symantec.de.