



MessageLabs Intelligence: September-Report und Analyse des 3. Quartals 2007

„Starker Anstieg der Viren- und Phishing-Aktivitäten im Gefolge der Storm Worm-Welle“

Einleitung

Herzlich willkommen zur neuesten Ausgabe des monatlichen Intelligence Reports von MessageLabs. In diesem Bericht informieren wir Sie über die aktuellen Gefahrentrends im September und dem dritten Quartal 2007, um Sie über die Entwicklung von Bedrohungen durch Viren, Spam und andere unwillkommene Online-Inhalte auf dem Laufenden zu halten.

Die wichtigsten Ergebnisse dieses Berichts in Kürze:

Spam-Quote – 73,5 Prozent im September (ein Rückgang um 0,5 Prozentpunkte gegenüber dem Vormonat).

Viren-Quote – Eine von 48,8 E-Mails war im Berichtsmonat mit einem Schadprogramm verseucht (ein Anstieg um 0,8 Prozentpunkte gegenüber dem Vormonat).

Phishing-Quote – Hinter einer von 87,2 E-Mails verbarg sich der Versuch, persönliche Authentisierungsdaten auszuspionieren (ein Anstieg um 0,6 Prozentpunkte gegenüber dem Vormonat).

Bedrohungen der alten Schule kehren pünktlich zu Beginn des neuen Schuljahres zurück

In letzter Zeit standen die Viren- und Phishing-Aktivitäten häufig im Schatten der besonders turbulenten, eskalierenden Spam-Aktivitäten. Im September änderte sich dies jedoch wieder. Die Viren-Quoten erreichten ein Niveau, das zuletzt vor mehr als 18 Monaten beobachtet worden war, und die Phishing-Quote war in diesem Monat sogar so hoch wie nie zuvor. Pünktlich zu Beginn des neuen Schuljahres kehrten also auch die Bedrohungen „der alten Schule“ wieder zurück.

Weitere Analysen der Viren-Aktivitäten brachten zum Vorschein, dass die Cyber-Kriminellen immer mehr dazu übergehen, Links zu Websites mit dem Schadcode in ihre Mails einzufügen, statt die Malware selbst in Form eines Anhangs mit einer ausführbaren Datei zu verschicken. Im dritten Quartal 2007 gehörten 35 Prozent der E-Mail-Gefahren dieser Gattung an, ein Anstieg um 14,8 Prozentpunkte gegenüber dem vorherigen Quartal, in dem diese Zahl noch 20,2 Prozent betragen hatte. Dieser Anstieg bereitete vor allem den Social Engineering-Angriffen den Weg, bei denen die Opfer mit falschen Versprechungen auf Websites mit dem Schadcode gelockt werden sollen. Noch im ersten Quartal 2007 betrug der Anteil derartiger Angriffe an der gesamten abgefangenen Malware nur ca. 3,3 Prozent.

Ein Name, den man nach wie vor im Zusammenhang mit dem Anstieg der Viren-Quoten nennen und für diesen verantwortlich machen muss, ist Storm – ein Name, der auch bei allen Analysen der Online-Gefahren des Jahres 2007 eine große Rolle spielen dürfte. Als Folge des großen Anstiegs der Aktivitäten des Storm-Botnets (am 15. August), an denen weltweit schätzungsweise 1,8 Millionen kompromittierte Rechner beteiligt waren, stieg das Spam-Aufkommen für viele Domains in der folgenden Woche (17. - 23. August) um bis zu 30 Prozentpunkte an, bevor es sich wieder in den üblichen Regionen einpendelte.



Phishing

Der Anstieg der Phishing-Aktivitäten äußerte sich im Vorfeld der Weihnachtssaison größtenteils in einem Anstieg der Intensität und Anzahl der Angriffe auf einige größere Ziele. Diese Angriffe wurden häufig über mehrere Tage durchgeführt, bevor die Online-Kriminellen den Schwerpunkt auf ein anderes Ziel verlagerten. Kombiniert mit dem Anstieg der kleineren Angriffe auf eine Reihe anderer Ziele führte dies dazu, dass die gesamten Phishing-Aktivitäten im September einen Höhepunkt erreicht haben. Die bislang höchsten Phishing-Quoten waren vorher im Januar 2007 beobachtet worden, als sich hinter einer von 93 E-Mails der Versuch verbarg, persönliche Authentisierungsdaten auszuspiionieren.

Einige dieser Angriffe übertrafen zahlenmäßig alle bisherigen Viren- und Trojaner-Angriffe. Viren- und Trojaner-Angriffe erfolgen häufig in kleineren Wellen, Phishing-Angriffe werden jedoch meist mit großen Mengen von Spam-Mails durchgeführt. Ein typischer großer Angriff umfasst 20.000 bis 80.000 E-Mails, und in einigen Fällen sind es sogar 200.000 oder mehr. Ein Angriff kleineren Ausmaßes setzt sich meist aus mehreren kleinen Wellen mit jeweils 1.000 bis 2.000 E-Mails zusammen, die sich am Ende zu einer Gesamtzahl von 5.000 bis 10.000 E-Mails summieren.

Die gestiegene Verfügbarkeit von Phishing-Kits und die zunehmende Nutzung aggressiver Phishing-Techniken wie Botnet- oder „Rock“-Phishing haben dazu geführt, dass die Bedrohungen durch diese Art von Angriffen drastisch gestiegen sind. Diese neuen Methoden ermöglichen das Hosting der Phishing-Sites in Botnets, deren IP-Adressen mithilfe von Fast-Flux-Techniken ständig verändert werden.

„Rock“-Phishing ist eine Technik, die zuerst im November 2005 beobachtet wurde und ihren Namen der Verwendung eines Phishing-Kits verdankt, das als „Rock Phish“-Kit bezeichnet wurde. Dieses spezielle Phishing-Kit wurde nur innerhalb einiger weniger, ausgewählter krimineller Vereinigungen verbreitet, aber einige ähnliche Toolkits waren auf dem Schwarzmarkt bald auch für eine breitere Masse erhältlich. Diese Kits erleichtern es technisch weniger versierten Cyber-Kriminellen, ausgereifte Angriffe durchzuführen. Sie ermöglichen den Angreifern, auf einem einzigen kompromittierten Computer innerhalb eines Botnets mehrere Phishing-Sites gleichzeitig zu hosten. Kombiniert mit der Verwendung von Fast-Flux-Netzwerken mit sich schnell ändernden DNS-Einträgen können diese Sites über das gesamte Botnet hinweg repliziert werden, wodurch es sehr viel schwieriger wird, sie zu identifizieren und auszuschalten. Verstärkt werden können die Angriffe außerdem durch die Verwendung vieler verschiedener Domains, die von den Kriminellen kontrolliert werden und in vielen verschiedenen Ländern über zahlreiche unterschiedliche Registrierungsorganisationen registriert sind.

Durch die Nutzung verschiedener Domains von unterschiedlichen Registrierungsorganisationen auf der ganzen Welt kann das Botnet einige Tage aktiv bleiben, da es bei einigen Domains länger dauert, sie abzuschalten. Das bedeutet, dass bei einem einzigen Phishing-Angriff während jeder Phase mehrere Tausend einzigartige Weblinks erzeugt werden können, bevor zu einem neuen Ziel übergegangen wird.

Jeder kompromittierte Computer innerhalb eines Botnets kann dazu verwendet werden, gleichzeitig mehrere Phishing-Sites zu hosten, die sich jeweils nur durch die Adresse oder Domain unterscheiden, die von dem Phishing-Angriff verwendet wird.

Aktien-Spam und Boardroom-Angriffe

Die meisten Menschen denken bei Spam vor allem an Mails, in denen ihnen Viagra oder gefälschte Uhren angeboten oder nach Art der Nigeria-Connection große Geldbeträge versprochen werden. In Wirklichkeit nehmen jedoch die Spam-Mails, bei denen im Rahmen so genannter „Pump-and-Dump“-Aktionen versucht wird, Aktienkurse zu manipulieren, mittlerweile Platz drei unter den häufigsten Spam-Arten ein. Aktien-Spam stellt eine große Gefahr dar, besonders weil die jüngsten Spam-



Aktionen über einen sehr kurzen Zeitraum in großem Umfang durchgeführt wurden und oft stark unkenntlich gemacht waren.

Zurzeit werden ca. 90 Prozent des Aktien-Spams als reine Textnachrichten ohne Bilder oder PDFs versendet. Ein Beispiel:

ola Noreen

This one will skyrocket,
tick-chvc
ask and check it out

Rhoda

S[tooo]ccc k F)D. E. G

Last 0.04

T:ar ge: t 0.12

R-umor N+e_w+s-:

Onco-logy M.e.d. I+n.c. . (.OTC: ONC-0) a Cancer Treatment Solutions Group is said to have experience double a 100% increase in revenue for the fiscal 3rd quarter ending July, 2007 compared with the prior year while fiscal fourth quarter results for 2007 are on track to exceed the year=92s third quarter results.

Diese Spam-Mail wurde in großen Mengen versendet. Zum Beispiel war ein Spam-Angriff, der am 20. September gestartet wurde, dafür verantwortlich, dass der E-Mail-Verkehr zu einigen Domains um das Dreifache anstieg. Nach dem ersten großen „Ausbruch“ der Spam-Mails verringert sich ihre Zahl, obwohl der Spam-Angriff noch einige Tage weitergeführt wird. Ein derart schneller Anstieg des E-Mail-Verkehrs könnte den Mailserver oder die Spamfilter-Appliance eines kleinen Unternehmens ohne weiteres außer Gefecht setzen.

Bei einem weiteren Angriff fing MessageLabs einige neue Vorschussbetrugsversuche nach Art der Nigeria-Connection ab, die über Kalender-Einladungen von Yahoo! Calendar verschickt wurden. Das folgende Beispiel wurde von MessageLabs Skeptic™ Radar abgefangen:

Subject: Be Our Representative. IP: 69.147.64.241 (n22.bullet.sp1.yahoo.com)
To: address-removed@#####.com From: calendar-invite@reply.yahoo.com

„Be Our Representative“ ist eine klassische Betreffzeile für diese Art von Spam, besonders beachtenswert ist jedoch die Absenderadresse: calendar-invite@reply.yahoo.com.

Eine Suche bei Google bringt schnell zum Vorschein, dass diese E-Mail-Adresse in den vergangenen Monaten auch für andere E-Mail-Betrugsversuche verwendet wurde.

Es sieht so aus, als haben die Vorschussbetrüger eine neue Möglichkeit gefunden, den Yahoo-Kalender auf dieselbe Weise zu missbrauchen, wie sie es zuvor bereits mit dem Adressbuch getan haben, d.h. durch Versenden von E-Mails mit Betreffzeilen wie „Ich habe eine neue E-Mail-Adresse“.



Add Event

Primary Information

Title:
max. 30/80 characters

Event Type:

Date:

Time: This is an **all day** event.
 Starts at:
Duration:

Location:

Notes:
max. 23/2000 characters

Weitere Analysen brachten außerdem zum Vorschein, dass es keine Höchstgrenze für die Anzahl der Personen gibt, die man zu einem „Event“ einladen kann:

Invitations [\[Hide\]](#)

Enter the email addresses of those you wish to send an email invitation, separated by commas.

[\[Insert from Address Book - Find Free Times\]](#)

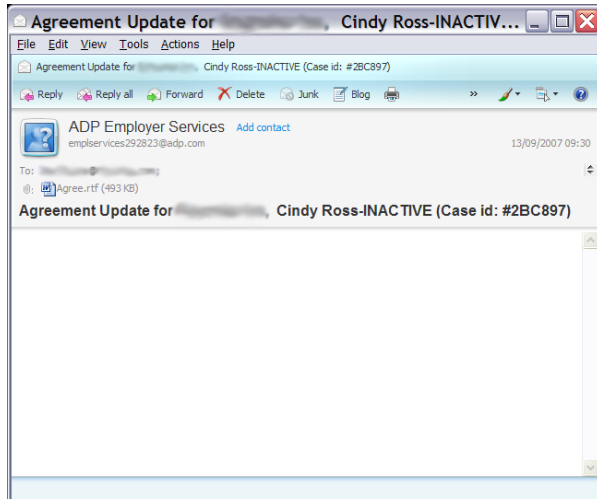
Note: These email addresses will be used to send an email invitation on your behalf and will not be collected or used by Yahoo! for any marketing purposes.

Zweite Welle der gezielten Angriffe auf Führungskräfte

Am 12. September fing MessageLabs mehr als 800 unterschiedliche E-Mail-Angriffe von derselben kriminellen Vereinigung ab, die für die Angriffe auf Führungskräfte und Mitglieder des oberen Managements verantwortlich war, von denen MessageLabs Ende Juni berichtet hatte (<http://www.messagelabs.com/resources/press/3845>).

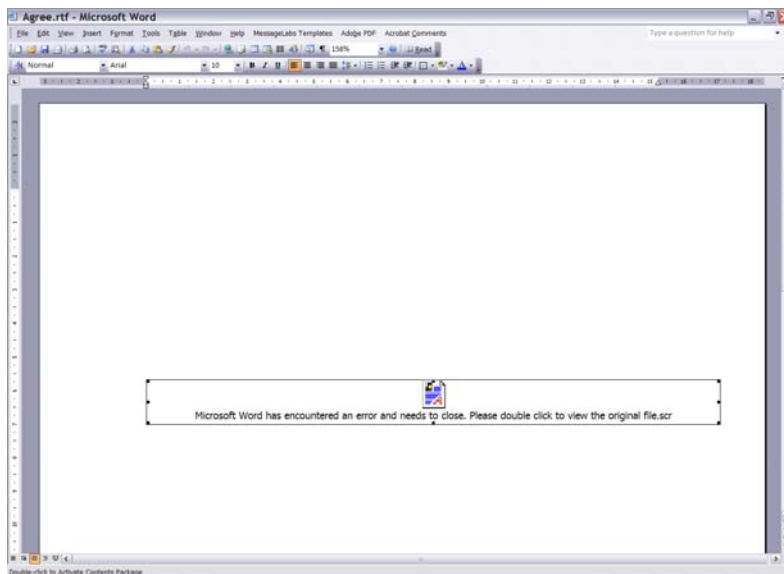
Drei separaten Angriffswellen, die am 12. September abgefangen wurden, folgte eine vierte Welle in den Morgenstunden des 13. September, die schließlich zu einer Gesamtzahl von mehr als 1.000 personalisierten E-Mail-Angriffen innerhalb von 16 Stunden führte.

Anders als bei den letzten Angriffen, bei denen der Name und die Position des Opfers in der Betreffzeile der E-Mail genannt wurden, schienen diese E-Mails von einer Personalvermittlung zu stammen und nannten im Betreff den Namen des Unternehmens der Zielperson:



Weitere Analysen der 1.100 Empfänger brachten zum Vorschein, dass die Angriffe sich wieder an Führungskräfte und Mitglieder des oberen Managements richteten, wobei auch versucht wurde, über mehrere Zielpersonen in ein Unternehmen zu gelangen.

Das Profil des Angriffs ähnelt dem vom 26. Juni, allerdings benutzten die Kriminellen dieses Mal noch ausgefeiltere Methoden. Keine der E-Mails beinhaltete einen Nachrichtentext. Der RTF-Anhang war der einzige Inhalt der E-Mails. Nach dem Öffnen sieht diese RTF-Datei folgendermaßen aus:



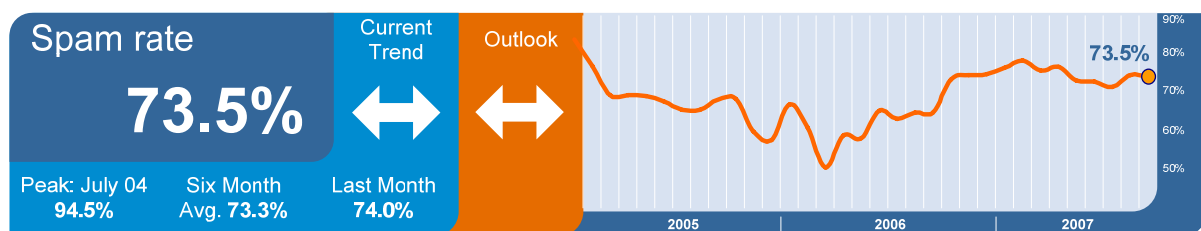
Die RTF-Datei enthält eine ausführbare Datei, die nach dem Öffnen zwei Dateien auf dem Rechner des Opfers ablegt. Diese wiederum laden eine Textdatei mit der Adresse einer weiteren Komponente herunter, die ebenfalls heruntergeladen und ausgeführt wird. Diese Komponente versucht dann, einen sicheren Verbindungskanal zu dem Server des Angreifers aufzubauen, um diesen für die Übermittlung sensibler Informationen an den Angreifer zu verwenden.



Weltweite Trends & Content-Analyse

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

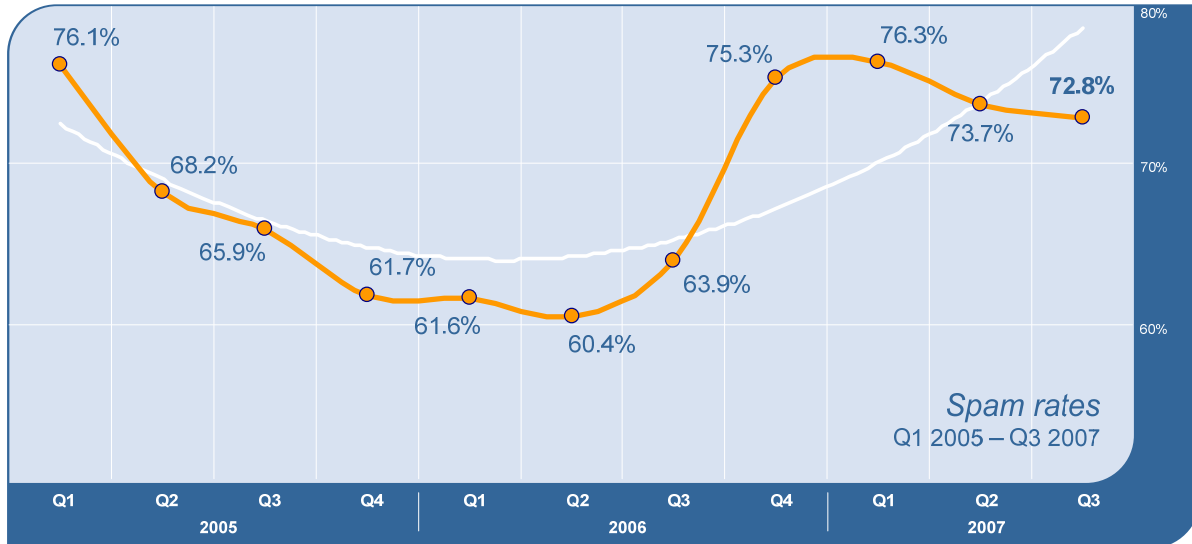
Spam-Schutz mit Skeptic™: Der Anteil von Spam am weltweiten, an gültige Empfänger adressierten E-Mail-Verkehr aus neuen oder unbekanntem Quellen belief sich im September 2007 auf 73,5 Prozent (oder 1 von 1,36 Mails). Das entspricht einem Rückgang um 0,5 Prozentpunkte gegenüber dem Vormonat.



Tatsächlich ist die offiziell gemessene Quote von 73,5 Prozent jedoch niedriger als der wahre Spam-Anteil am E-Mail-Verkehr. Denn mittels Traffic-Management kann MessageLabs mittlerweile exakt kontrollieren, welche Bandbreite jenen Spam-Nachrichten zugewiesen wird, die zweifellos schädlichen Ursprungs sind. So lassen sich die jeweiligen Verbindungen auf Schneckentempo drosseln, um Spammern den Eindruck zu vermitteln, dass sie mit einem sehr langsamen Modem kommunizieren.

Dies macht es für Spammer unglaublich mühsam, ihre Spam-Mails an Kunden von MessageLabs zu versenden, da das Traffic Management die Spam-Mails recht effektiv in ihre Netzwerke zurückschiebt und das schnelle Aussenden großer Mengen von Spams verhindert. Diese Vorgehensweise führt schließlich dazu, dass viele dieser Verbindungen aufgrund einer „Zeitüberschreitung“ abgebrochen werden oder zu schwächeren Zielen übergehen. Wenn man zum Vergleich die Anzahl der Spams heranzieht, die bei den ungeschützten Honey-Pots von MessageLabs ankommen, ist davon auszugehen, dass die „echte“ Spam-Quote eher im Bereich von 85,6 Prozent liegt, was einem Anstieg um 1,9 Prozentpunkte seit August entspräche. Weitere Informationen zu dieser Methode finden Sie weiter unten in diesem Bericht im Abschnitt „Traffic-Management“.

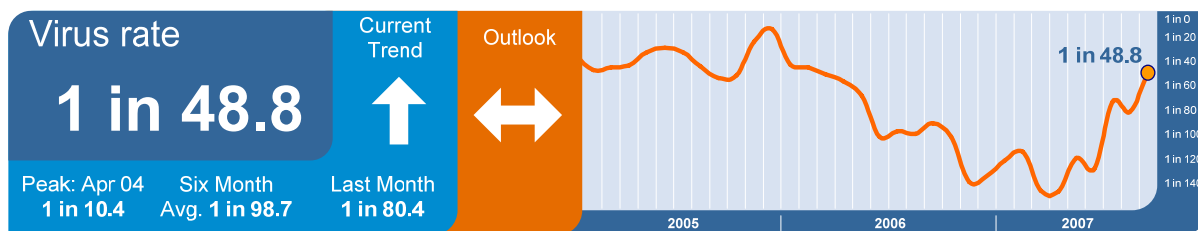
Quartalsanalyse: Aus der unten gezeigten Grafik wird ersichtlich, dass die von MessageLabs im dritten Quartal 2007 abgefangene Spam-Quote etwas höher ist als in den dritten Quartalen der Jahre 2006 und 2005.



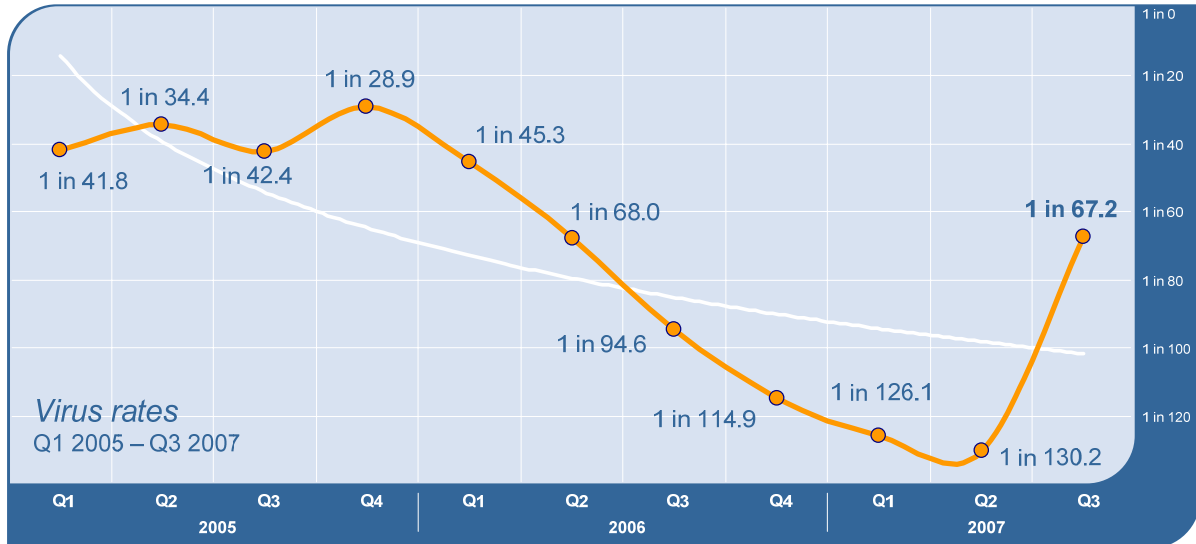
Seit Ende 2006 und der zunehmenden Nutzung von neuen, robusteren Botnet-Technologien zum Beispiel in Form der WarezoV- und Storm-Botnets haben sich die Spam-Quoten relativ konstant auf einem hohen Niveau gehalten, das in etwa dem Niveau von Anfang 2005 entspricht.

Die jüngsten Botnets sind sehr viel widerstandsfähiger gegenüber Unterbrechungen und Störungen als ihre Vorgänger. Mit ihrer Fähigkeit, sich nach Störungen zu regenerieren, sind sie fast in der Lage, „sich selbst zu heilen“ und sich außerdem mit DDoS-Angriffen zu verteidigen, wenn sie merken, dass sie ausspioniert werden. Traditionelle Gegenmaßnahmen sind gegen diese neue Art von Botnets nicht sehr effektiv, so dass es nötig wurde, neue Methoden zu entwickeln. Es dürfte daher nur noch eine Frage der Zeit sein, bis man die Verantwortlichen identifizieren und zur Rechenschaft ziehen kann.

Viren- und Trojaner-Abwehr mit Skeptic™: Der Anteil der virenverseuchten E-Mails am weltweiten, an gültige Empfänger adressierten E-Mail-Verkehr stieg im September gegenüber dem Vormonat um 0,8 Prozentpunkte auf 2,05 Prozent. Eine von 48,8 an gültige Empfängeradressen gerichteten E-Mails aus neuen oder bislang unbekanntem zweifelhaften Quellen war verseucht.



Quartalsanalyse: Seit 2006 sind die Viren- und Trojaner-Quoten relativ kontinuierlich gesunken. Im dritten Quartal 2007 nahm dieser Abwärtstrend jedoch ein Ende. Eine von 67,2 E-Mails war im dritten Quartal 2007 verseucht – dies entspricht der höchsten Quartalsquote seit dem 1. Quartal 2006.

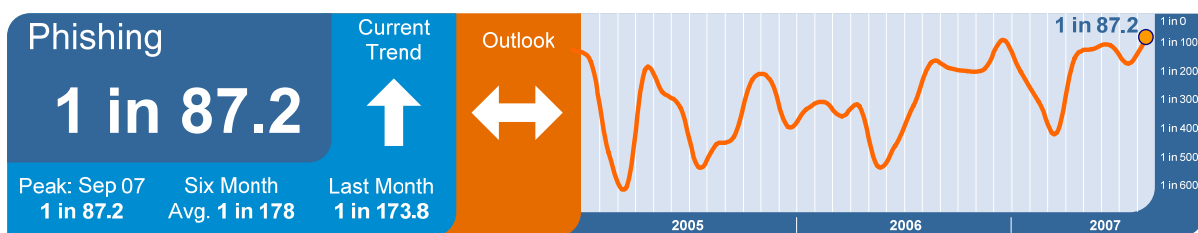


Im dritten Quartal 2007 bestanden 35 Prozent der E-Mail-Gefahren in dieser Kategorie zumeist aus Mails, die Links zu Websites enthielten, auf denen der Schadcode gehostet war. Gegenüber der Zahl von 20,2 Prozent im vorherigen Quartal nahm diese Art von Gefahren also um 14,9 Prozentpunkte zu. Zumeist handelte es sich dabei um Social-Engineering-Angriffe, bei denen die Angreifer die Empfänger der E-Mails dazu verleiten wollten, Links zu den Websites mit ihrem Schadcode anzuklicken. Im ersten Quartal 2007 hatte diese Zahl noch ca. 3,3 Prozent der gesamten abgefangenen Malware betragen.

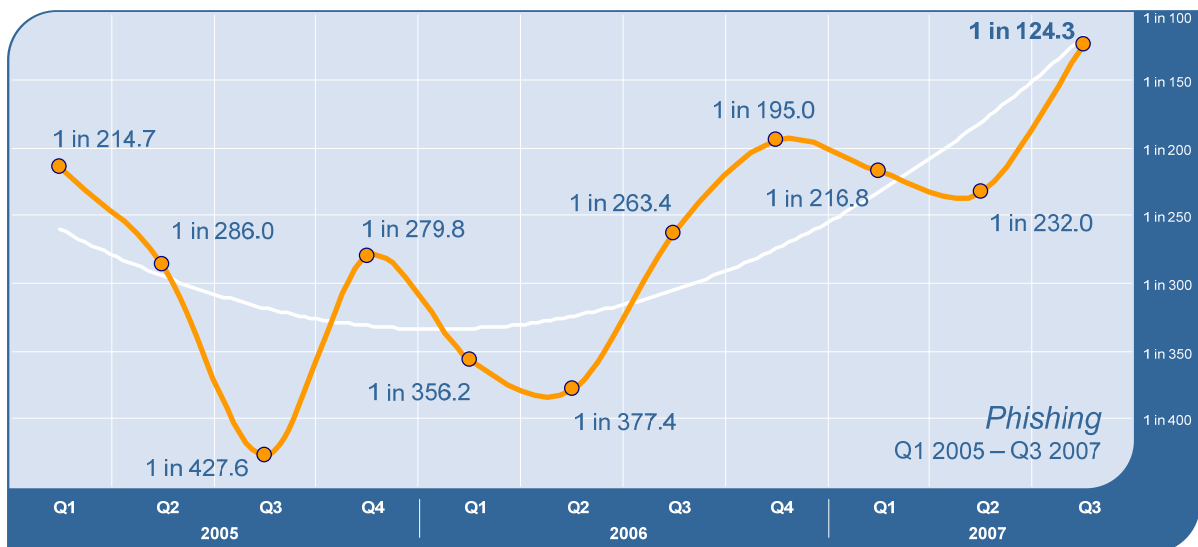


Phishing: Im September stieg die Phishing-Quote gegenüber dem Vormonat um 0,6 Prozentpunkte auf 1,15 Prozent. Hinter einer von 87,2 E-Mails verbarg sich der Versuch, persönliche Authentisierungsdaten auszuspionieren - dies ist die höchste Quote, die jemals erfasst wurde. Zuvor hatten die Phishing-Angriffe ihren vorläufigen Höhepunkt im Januar 2007 gehabt, als die Quote auf 1 zu 93,3 gestiegen war.

Der Anteil von Phishing-Mails an allen per E-Mail verbreiteten Gefahren einschließlich Viren und Trojanern stieg gegenüber dem Vormonat um 9,7 Prozentpunkte auf 56,0 Prozent aller mit betrügerischer Absicht versendeten E-Mails, die MessageLabs im September abgefangen hat.



Quartalsanalyse: Die durchschnittliche Phishing-Quote lag im dritten Quartal bei einer von 124,3 E-Mails und ist damit die höchste Quote, die jemals in einem Quartal beobachtet wurde.



Insgesamt machten die Phishing-Aktivitäten in diesem Quartal 54,5 Prozent der Malware-Bedrohungen aus, ein Rückgang um 9,3 Prozentpunkte gegenüber dem vorherigen Quartal. Im selben Zeitraum 2006 lag diese Quote bei 35,9 Prozent.



Skeptic™ Web Security Services Version 2.0: Version 2.0 der Web Security Services, die auf der proprietären Skeptic-Technologie von MessageLabs basieren, ermöglicht MessageLabs, die neuesten Bedrohungs- und Reputationsinformationen von anderen Protokollen (wie z.B. E-Mail) zu erfassen und dieses Wissen auf den Web-Traffic anzuwenden.

Werbung und Popups waren im September mit 43,66 Prozent (ein Rückgang um 1,4 Prozentpunkte gegenüber August) die häufigsten Auslöser für die richtlinienbasierte Filterung, die MessageLabs für seine Geschäftskunden durchführt. Die Kategorie „Unclassified“ enthält neue und zuvor nicht kategorisierte Sites, die möglicherweise gesperrt werden müssen. Diese Kategorie zeichnete für 14,04 Prozent des abgefangenen Web-Traffic verantwortlich.

Diese Filterung dieser Kategorie verbessert den Schutz vor so genannten Domain-Kiting-Sites, die innerhalb eines Zeitraums von 24 bis 48 Stunden auftauchen und wieder verschwinden – denn solche Sites können für kriminelle Zwecke verwendet werden und z.B. als Phishing- und Spam-Sites dienen, mithilfe von Trojanern Informationen stehlen oder für andere betrügerische Aktivitäten genutzt werden. 59,2 Prozent der webbasierten Viren wurden dieser Kategorie zugeordnet, ebenso wie 84,0 Prozent der Spyware, Adware und anderer potenziell unerwünschter Programme.

Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	43.66%	Winfixer	15.73%	PUP-SaveNow	96.98%
Unclassified	14.04%	Suspicious IFrame.b	10.26%	PUP-GAIN	1.55%
Streaming Media	11.07%	Exploit-ANIfile.c	6.34%	PUP-ZangoSA	0.46%
Chat	9.24%	VBS/Psyme	5.48%	PUP-MediaTickets	0.31%
Personals & Dating	4.41%	W32/Winko.wormlcfg	4.52%	PUP-Boran	0.12%
Adult/Sexually Explicit	3.17%	Tool-TFTPD32	4.24%	PUP-ISTBar	0.12%
Photo Searches	2.06%	Trojan-Downloader.VBS.Agent.n	3.69%	PUP-Coolsavings	0.08%
Downloads	2.03%	Trojan-Downloader.VBS.Small.co	3.30%	PUP-TCent	0.08%
Web-based E-mail	1.88%	Trojan-PSW.Win32.OnLineGames.aci	2.13%	PUP-2Search	0.04%
Spyware	1.70%	JS/Exploit-DDay	2.07%	PUP-Zeno	0.04%

Die Analysen zeigen außerdem, dass 99,9 Prozent der Abfangaktivitäten aufgrund von Regeln erfolgten, die von Richtlinien ausgelöst wurden, die von Systemadministratoren implementiert wurden.

Weitere Analysen zeigen, dass 15,1 Prozent der im September abgefangenen Malware neuer Herkunft war. Das zunehmende Auftreten von immer mehr Arten zuvor unbekannter Malware lässt vermuten, dass es für die herkömmlichen Methoden immer schwieriger werden wird, ausreichenden Schutz vor einer sich derart schnell verändernden Bedrohungslandschaft zu bieten.

MessageLabs hat im September täglich ca. 668 neue Sites identifiziert, die Malware oder potenziell unerwünschte Inhalte einschließlich Spy- und Adware beherbergten.



Die folgende Tabelle zeigt, welchen Kategorien die Sites angehörten, die MessageLabs für Unternehmen verschiedener Größen blockiert hat:

	Total	1-500	501-2500	2500+
Advertisements & Popups	48.50%	55.32%	48.12%	20.02%
Streaming Media	13.77%	16.37%	10.98%	6.30%
Chat	8.97%	5.89%	24.33%	2.36%
Personals & Dating	5.67%	2.78%	0.84%	24.12%
Adult/Sexually Explicit	4.19%	1.44%	1.76%	19.00%
Web-based E-mail	2.52%	3.80%	0.25%	0.00%
Downloads	2.48%	3.77%	0.05%	0.12%
Spyware	2.22%	0.95%	2.99%	6.64%
Photo Searches	2.10%	2.67%	0.81%	1.31%
Other categories	1.52%	1.24%	2.51%	1.47%
Unclassified	1.48%	1.19%	3.47%	0.17%
Gambling	1.31%	0.50%	0.84%	5.38%
Proxies & Translators	1.31%	0.06%	0.19%	8.06%
Entertainment	0.89%	1.27%	0.28%	0.08%
Infrastructure	0.88%	0.77%	1.26%	0.82%
Blogs & Forums	0.53%	0.66%	0.54%	0.00%
Games	0.49%	0.32%	0.07%	1.75%
Shopping	0.49%	0.66%	0.29%	0.00%
Tasteless & Offensive	0.32%	0.20%	0.24%	0.97%
Ringtones/Mobile Phone Downloads	0.22%	0.07%	0.10%	1.00%
Spam URLs	0.12%	0.06%	0.06%	0.43%

Top 5

Besondere Beachtung sollte der Tatsache geschenkt werden, dass Social-Networking-Sites wie FaceBook und MySpace der Kategorie „Personals & Dating“ angehören und den Großteil der geblockten Sites in dieser Kategorie ausmachen.

Ein durchschnittliches Unternehmen mit bis zu 500 Mitarbeitern kann damit rechnen, pro Tag 10 Zugriffsversuche auf Social-Networking-Sites blockieren zu müssen, verglichen mit über 850 bei einem Unternehmen mit 2.500 oder mehr Mitarbeitern.

Die weitere Analyse der Kategorie „Personals & Dating“ offenbart die folgende Aufschlüsselung der Top 5 für die verschiedenen Unternehmensgrößen:

Bis 500 Mitarbeiter

- FaceBook
- Ning
- Friends Reunited
- Faceparty
- MySpace

500 – 2.500 Mitarbeiter

- Friends Reunited
- Faceparty
- Hi5
- Match
- Keen
- ...
- MySpace (#7)
- FaceBook (#10)

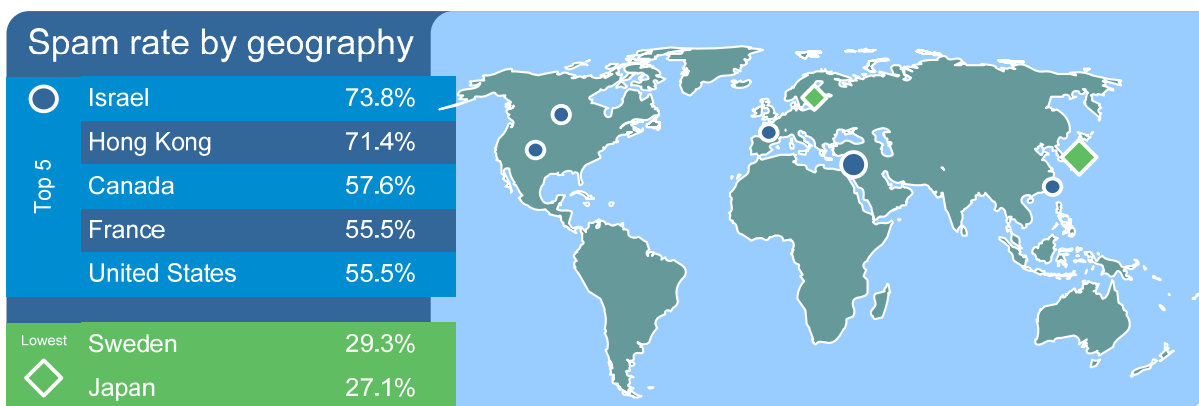
Mehr als 2.500 Mitarbeiter

- FaceBook
- MySpace
- Rsvp
- Faceparty
- Hi5

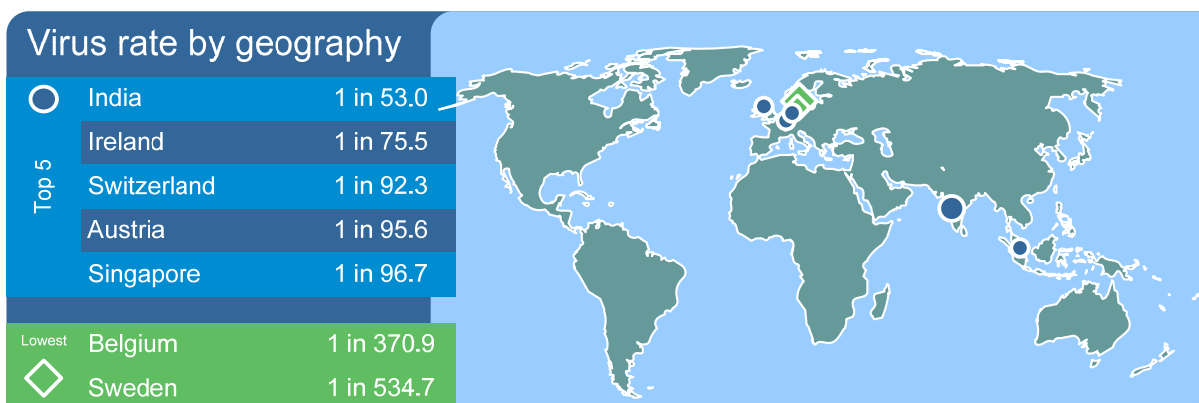


Online-Gefahren nach Zielländern

Monats-Analyse: Soweit dies möglich ist, analysiert MessageLabs die geografische Verteilung des E-Mail-Verkehrs und gewinnt auf diese Weise Daten zu den regionalen Auswirkungen von Spam und Viren sowie zu der Anfälligkeit der verschiedenen Länder für diese Gefahren. Die folgenden Grafiken zeigen die Auswirkungen und Quoten für die einzelnen Länder im September 2007.



Israel behält auch im September seine Position an der Spitze der Spam-Charts, den stärksten Anstieg der Spam-Belastung innerhalb der Top 5 verzeichnete jedoch Kanada mit 7,3 Prozentpunkten. Mit einem Anstieg der Spam-Quote um 12,6 Prozentpunkte gab es in Italien den stärksten Anstieg insgesamt. Der größte Rückgang wurde in Deutschland beobachtet, wo die Spam-Quote um 10,2 Prozentpunkte auf 58,5 Prozentpunkte sank, woraufhin Deutschland im September die Top 5 der Länder mit der höchsten Spam-Belastung verlassen hat.



Die Virenaktivitäten gingen in Indien zwar um 1,7 Prozentpunkte zurück, aber dennoch bleibt Indien weiterhin das Land mit der höchsten Viren-Quote. Den größten Anstieg der Viren-Aktivitäten verzeichneten die Niederlande, und zwar um 0,20 Prozentpunkte. Statt wie im August eine von 750,1 E-Mails war dort im September eine von 303,3 E-Mails mit einem Virus verseucht.

Detaillierte Zahlen zu den aktuellen Online-Gefahren nach Zielländern finden Sie im Anhang.



Quartalsanalyse: Die unten abgebildeten Charts veranschaulichen die interessanten Erkenntnisse, die sich durch den Vergleich der Änderungen von Quartal zu Quartal gewinnen lassen.

Spam-Quoten nach Ländern (pro Quartal)

	2005				2006				2007		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Australia	37.96%	40.15%	40.02%	39.50%	39.97%	44.84%	46.11%	57.02%	47.43%	36.30%	37.10%
Austria	54.64%	50.74%	50.88%	48.49%	43.61%	43.92%	55.50%	55.88%	48.33%	46.83%	44.73%
Belgium	53.13%	52.87%	57.72%	57.04%	50.61%	44.43%	50.08%	60.26%	47.20%	45.07%	48.10%
Canada	82.52%	77.08%	73.46%	64.71%	57.63%	43.17%	52.61%	59.84%	55.47%	45.90%	49.77%
China	19.38%	26.76%	30.66%	30.36%	30.02%	37.49%	44.69%	48.18%	48.67%	34.05%	51.75%
France	48.57%	50.51%	52.47%	47.87%	42.38%	40.13%	53.50%	57.72%	55.37%	51.33%	54.00%
Germany	74.50%	67.58%	64.89%	60.80%	53.62%	49.18%	57.48%	67.57%	60.63%	60.53%	53.90%
Hong Kong	63.89%	59.01%	62.68%	64.92%	78.59%	68.09%	63.89%	69.41%	65.63%	59.73%	65.30%
India	84.87%	81.72%	81.75%	84.95%	77.54%	19.36%	27.40%	43.95%	44.63%	35.57%	32.90%
Ireland	67.60%	69.26%	66.05%	65.71%	57.10%	48.36%	66.08%	65.36%	49.40%	53.63%	49.93%
Israel	69.62%	73.07%	72.61%	71.61%	67.22%	69.70%	76.83%	78.97%	66.70%	65.23%	68.43%
Italy	65.20%	60.57%	62.31%	61.15%	59.84%	53.35%	51.45%	59.45%	62.50%	41.27%	38.93%
Japan	9.67%	31.08%	36.61%	32.23%	24.25%	27.10%	29.55%	34.17%	33.77%	32.43%	24.93%
Netherlands	44.79%	47.46%	52.40%	47.96%	46.00%	42.61%	50.83%	53.77%	40.90%	33.83%	34.03%
Singapore	26.66%	36.12%	35.78%	37.00%	39.54%	39.54%	52.24%	63.98%	54.80%	36.13%	43.57%
Spain	35.02%	39.94%	43.59%	47.65%	40.25%	32.67%	42.61%	41.18%	43.83%	42.03%	38.57%
Sweden	37.11%	48.32%	45.34%	41.16%	36.87%	35.88%	43.22%	46.09%	39.40%	37.27%	29.73%
Switzerland	77.21%	72.44%	75.54%	62.15%	32.46%	33.57%	41.36%	52.93%	49.93%	43.17%	42.93%
United Arab Emirates	66.16%	61.04%	54.26%	48.68%	48.94%	48.78%	57.65%	61.53%	54.23%	42.13%	37.77%
United Kingdom	67.58%	59.34%	56.88%	56.80%	54.05%	51.18%	52.49%	58.75%	49.53%	42.07%	41.90%
United States	85.63%	79.43%	74.56%	64.84%	61.10%	55.12%	61.84%	69.90%	61.60%	49.87%	52.17%



Viren-Quoten nach Ländern (pro Quartal)

	2005				2006				2007		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Australia	4.87%	5.35%	3.33%	5.73%	2.33%	1.09%	0.77%	1.29%	0.80%	0.40%	0.58%
Austria	5.15%	4.86%	3.27%	8.69%	2.41%	1.20%	1.03%	0.79%	1.08%	1.19%	1.82%
Belgium	4.70%	3.55%	2.98%	3.82%	1.94%	0.99%	0.59%	0.38%	0.56%	0.33%	0.42%
Canada	1.26%	1.80%	1.31%	4.22%	2.12%	1.74%	0.92%	0.63%	0.62%	0.63%	1.11%
China	21.12%	18.13%	15.10%	13.46%	6.12%	1.82%	1.97%	1.76%	0.94%	1.77%	1.59%
France	6.72%	4.25%	3.22%	5.72%	3.18%	2.38%	2.09%	1.78%	2.41%	1.22%	1.48%
Germany	4.50%	4.64%	3.55%	8.49%	3.18%	2.54%	3.30%	2.28%	2.66%	1.88%	1.99%
Hong Kong	6.35%	7.94%	6.46%	7.13%	2.68%	1.93%	2.00%	1.47%	1.06%	1.40%	1.92%
India	2.62%	4.70%	3.24%	2.87%	3.82%	10.80%	7.77%	4.42%	2.94%	3.14%	3.59%
Ireland	14.53%	6.97%	6.32%	7.24%	3.27%	1.83%	2.64%	3.05%	2.08%	1.27%	1.44%
Israel	13.35%	7.82%	4.51%	5.98%	2.72%	1.56%	0.91%	0.57%	0.48%	0.97%	1.02%
Italy	11.58%	7.24%	4.65%	5.38%	2.37%	1.42%	1.89%	0.80%	0.81%	1.60%	1.40%
Japan	3.25%	6.22%	5.43%	4.91%	2.72%	1.48%	1.28%	0.85%	0.55%	0.44%	0.71%
Netherlands	4.30%	3.25%	2.02%	3.52%	1.76%	1.22%	0.94%	0.54%	0.51%	0.33%	0.33%
Singapore	9.88%	11.18%	8.58%	11.93%	6.33%	4.27%	2.50%	1.45%	1.10%	1.32%	1.73%
Spain	19.21%	9.17%	6.59%	6.84%	5.10%	3.24%	2.93%	1.32%	1.45%	1.04%	1.07%
Sweden	3.91%	1.40%	1.22%	2.36%	1.17%	0.74%	1.01%	0.70%	0.47%	0.23%	0.23%
Switzerland	2.41%	3.82%	2.11%	4.51%	2.82%	1.76%	1.42%	1.15%	1.40%	1.57%	2.25%
United Arab Emirates	5.19%	8.25%	8.81%	13.69%	6.84%	4.35%	3.09%	1.52%	1.15%	1.63%	2.14%
United Kingdom	2.29%	2.97%	2.11%	3.32%	1.79%	1.17%	0.98%	0.97%	0.77%	0.71%	1.10%
United States	2.11%	2.43%	2.16%	5.59%	2.40%	1.81%	1.09%	0.64%	0.75%	0.80%	1.14%

Online-Gefahren nach Zielbranchen

Monats-Analyse: Sofern möglich, analysiert MessageLabs den E-Mail-Verkehr verschiedener Branchen und ermittelt, wie stark die größten Wirtschaftssektoren von Spam und Viren betroffen und für diese unerwünschten E-Mails anfällig sind. Die folgenden Grafiken zeigen die Auswirkungen und Quoten für die einzelnen Branchen im September 2007.

Spam rate by vertical			Virus rate by vertical		
Top 5	Agriculture	67.8%	Education	1 in 47.7	
	Telecoms	67.2%	Wholesale	1 in 94.6	
	Manufacturing	60.9%	Accom/Catering	1 in 101.4	
	Education	58.2%	Gov/Public Sector	1 in 106.0	
	Wholesale	57.7%	Retail	1 in 108.3	
Lowest	Estate Agents	35.1%	Telecoms	1 in 311.9	
	Finance	33.8%	Agriculture	1 in 394.1	

Die Spam-Quoten sind im September in allen Branchen gestiegen, wobei das Gesundheitswesen mit einem Anstieg um 7,8 Prozentpunkte die höchste Zunahme der Spam-Belastung verzeichnete. Die Landwirtschaft bleibt nach einem Anstieg um 0,9 Prozentpunkte seit August auch im September der Sektor mit der höchsten Spam-Quote.

Der Bildungssektor nimmt weiterhin die Spitzenposition der Viren-Charts ein, obwohl die Viren-Quote in diesem Sektor seit August um 0,25 Prozentpunkte gesunken ist. Diese Entwicklung scheint für den Bildungssektor zu dieser Jahreszeit typisch und durch die langen Sommer- bzw. Semesterferien bedingt zu sein.

Detaillierte Zahlen zu den aktuellen Online-Gefahren nach Zielbranchen finden Sie im Anhang.



Quartalsanalyse: Die unten abgebildeten Charts veranschaulichen die interessanten Erkenntnisse, die sich durch den Vergleich der Änderungen von Quartal zu Quartal für die Jahre 2005 bis 2007 gewinnen lassen.

Spam-Quoten nach Branchen (pro Quartal)

	2005				2006				2007		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Accom/Catering	52.95%	53.73%	50.03%	46.16%	41.69%	42.94%	52.66%	63.71%	52.03%	39.07%	36.73%
Agriculture	76.83%	71.72%	64.34%	59.32%	48.47%	45.50%	56.15%	60.53%	53.37%	60.73%	67.17%
Building/Cons	70.42%	66.41%	62.61%	54.73%	46.03%	43.14%	49.70%	54.33%	43.97%	34.93%	33.90%
Business Support Services	51.27%	47.75%	45.54%	45.69%	51.29%	60.72%	59.22%	69.71%	53.10%	47.20%	40.07%
Chem/Pharm	81.81%	73.34%	75.47%	69.52%	65.56%	60.87%	59.34%	63.19%	56.47%	45.43%	47.93%
Education	74.33%	66.13%	65.97%	68.47%	61.41%	61.01%	66.27%	72.87%	63.90%	55.40%	56.70%
Estate Agents	77.30%	73.38%	67.72%	63.82%	56.50%	48.92%	55.21%	55.08%	40.17%	36.03%	33.67%
Finance	66.01%	60.31%	58.95%	54.70%	49.68%	41.46%	47.66%	52.59%	41.13%	30.00%	31.20%
General Services	68.87%	67.87%	64.82%	58.48%	52.06%	46.74%	46.71%	54.77%	41.90%	37.20%	40.13%
Gov/Public Sector	49.51%	51.20%	48.54%	44.96%	40.71%	36.42%	39.91%	49.24%	43.13%	38.30%	39.77%
Health Care	84.62%	82.38%	76.33%	63.30%	54.25%	50.56%	56.77%	63.24%	54.77%	47.70%	49.43%
IT Services	83.45%	79.34%	71.16%	69.45%	63.87%	55.89%	54.93%	69.57%	60.63%	52.20%	51.50%
Manufacturing	78.23%	70.96%	63.79%	54.75%	59.10%	57.17%	63.37%	72.61%	66.93%	56.87%	58.33%
Marketing/Media	72.00%	64.99%	63.45%	62.58%	58.74%	54.30%	58.40%	64.17%	59.00%	50.70%	53.00%
Mineral/Fuel	75.49%	63.20%	60.23%	55.84%	48.70%	42.86%	53.96%	58.31%	51.73%	44.93%	39.87%
Non-Profit	62.98%	60.42%	58.00%	55.84%	48.89%	47.21%	54.49%	58.51%	48.10%	39.80%	46.07%
Prof Services	76.22%	70.05%	67.29%	61.18%	57.51%	52.25%	56.92%	64.66%	53.93%	44.10%	44.70%
Recreation	72.78%	67.17%	66.73%	64.78%	65.99%	62.50%	61.66%	59.40%	49.17%	40.33%	38.90%
Retail	76.29%	69.54%	67.12%	60.90%	61.61%	51.24%	57.15%	64.61%	56.27%	44.37%	44.93%
Telecoms	83.45%	81.41%	80.44%	70.53%	59.14%	54.89%	61.24%	65.60%	55.80%	41.07%	58.03%
Transport/Util	73.92%	64.87%	61.48%	61.32%	57.21%	49.08%	59.57%	64.96%	50.97%	47.33%	40.87%
Wholesale	81.94%	64.59%	62.51%	48.67%	50.74%	47.19%	57.82%	61.69%	57.77%	50.80%	51.80%



Viren-Quoten nach Branchen (pro Quartal)

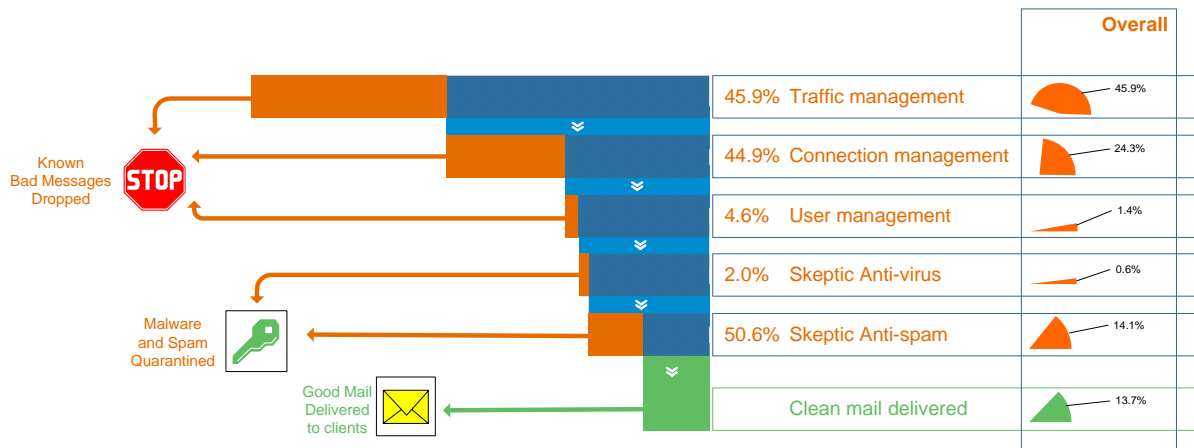
	2005				2006				2007		
	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3
Accom/Catering	7.36%	6.28%	4.46%	7.41%	3.46%	2.07%	1.60%	0.95%	1.11%	0.62%	1.30%
Agriculture	2.60%	2.27%	1.97%	3.38%	1.65%	0.97%	0.74%	0.45%	0.49%	0.28%	0.28%
Building/Cons	2.06%	2.15%	1.93%	3.55%	1.62%	0.95%	0.94%	0.80%	0.57%	0.46%	0.77%
Business Support Services	12.81%	17.76%	12.27%	12.57%	13.55%	12.39%	7.51%	2.13%	1.50%	0.63%	0.52%
Chem/Pharm	1.35%	3.35%	1.52%	2.56%	1.24%	0.91%	0.93%	0.74%	0.98%	1.29%	1.91%
Education	4.48%	4.24%	3.89%	4.28%	2.91%	2.06%	1.98%	1.73%	1.66%	1.26%	2.32%
Estate Agents	2.06%	2.07%	1.71%	2.98%	1.19%	0.75%	0.57%	0.40%	0.58%	0.74%	0.90%
Finance	2.01%	2.37%	1.58%	3.72%	1.27%	0.80%	0.85%	0.96%	0.70%	0.75%	0.79%
General Services	3.73%	3.69%	2.59%	4.01%	1.99%	1.07%	0.92%	0.89%	0.78%	0.53%	0.76%
Gov/Public Sector	4.57%	3.08%	2.34%	3.98%	2.02%	1.37%	1.25%	1.00%	0.82%	0.63%	0.91%
Health Care	1.52%	1.74%	1.38%	3.49%	1.50%	1.01%	0.72%	0.64%	0.74%	0.62%	0.96%
IT Services	1.35%	1.68%	1.41%	3.55%	3.24%	0.97%	0.64%	0.55%	0.71%	0.82%	1.23%
Manufacturing	4.51%	3.92%	3.72%	7.99%	3.17%	2.41%	1.47%	1.02%	0.98%	0.89%	1.17%
Marketing/Media	2.54%	2.91%	2.31%	3.30%	1.77%	1.21%	1.05%	0.90%	0.96%	0.80%	1.17%
Mineral/Fuel	2.89%	3.48%	2.91%	5.13%	2.81%	1.60%	1.31%	0.86%	0.74%	0.61%	1.06%
Non-Profit	3.78%	3.76%	3.14%	5.13%	3.11%	1.98%	1.49%	0.97%	0.82%	0.58%	0.98%
Prof Services	1.43%	2.48%	2.24%	6.60%	2.03%	1.17%	0.88%	0.68%	0.84%	0.82%	1.37%
Recreation	3.35%	4.05%	3.31%	4.42%	2.09%	1.24%	0.93%	0.87%	0.68%	0.72%	0.81%
Retail	2.57%	3.30%	2.58%	4.79%	1.67%	1.16%	0.98%	0.75%	0.91%	1.04%	1.53%
Telecoms	0.99%	0.84%	0.60%	1.46%	0.75%	0.53%	0.46%	0.30%	0.23%	0.18%	0.34%
Transport/Util	3.54%	3.46%	3.03%	4.65%	2.30%	1.37%	1.07%	0.74%	0.52%	0.51%	0.92%
Wholesale	4.40%	5.85%	3.02%	5.26%	6.04%	4.82%	2.98%	1.55%	1.14%	1.15%	1.43%



Traffic-Management (auf Protokollebene)

Anwendungen zum Management des E-Mail-Verkehrs senken weiterhin das Gesamtvolumen der übermittelten Nachrichten durch Techniken, die auf Protokoll-Ebene aktiv sind. Dazu zählen Verfahren zur Identifikation gesperrter Absender und zur gezielten Verlangsamung von Mail-Server-Verbindungen über Funktionen, die in das TCP-Protokoll eingebettet sind. Auf diese Weise erreichen deutlich weniger bekannte Spam-Formen ihre Adressaten, während die reibungslose Übermittlung aller zulässigen E-Mails gewährleistet bleibt.

Im September 2007 hat MessageLabs durchschnittlich 2,84 Milliarden SMTP-Verbindungen pro Tag verarbeitet, von denen 90,8 Prozent im Zuge des Traffic-Managements und dessen Protokoll-Monitorings gedrosselt wurden, weil es sich um eindeutig schädlichen und unerwünschten E-Mail-Verkehr handelte. Vom übrigen Web-Traffic getrennt, werden diese Verbindungen gezielt mit den Kontroll- und Steuerungsinstrumenten von MessageLabs Connection Management und MessageLabs Skeptic™ verarbeitet.



Verbindungs-Management

Das Verbindungs-Management erweist sich als ein sehr effektives Instrument, um insbesondere eine Adressbücher-Plünderung, Brute-Force-Angriffe und E-Mail-basierende Denial-of-Service-Angriffe zu stoppen – also solche Hacker-Praktiken, bei denen unerwünschte Massenmails ein Unternehmen überfluten und auf diese Weise dessen Geschäftstätigkeit nachhaltig stören sollen.

Anwendungen für das Verbindungs-Management arbeiten auf SMTP-Ebene und nutzen Techniken, die überprüfen, inwieweit aufzubauende Mail-Server-Verbindungen tatsächlich erlaubt sind.

Eine *SMTP-Validierung* erkennt unerwünschte E-Mails von Urhebern, die für den Versand von Spam und Viren bekannt sind. Das Verfahren identifiziert solche Quellen als offene Proxy-Speicher ebenso eindeutig wie als Botnet und weist dann im Falle des Falles die Verbindungsabfrage entsprechend zurück. Im September hat MessageLabs auf diese Weise durchschnittlich 44,9 Prozent aller eingehenden Mails abgefangen, da diese aus Botnets oder anderen bekannten Schadprogramm-Quellen stammten.

Eine *Adress-Prüfung der registrierten Anwender* senkt die Gesamtmenge an E-Mails, die an registrierte Domains adressiert sind. Denn das Verfahren verwirft alle Verbindungen, die an ungültige oder nicht existierende Einzelempfänger gerichtet sind. Im September hat MessageLabs so durchschnittlich 4,6 Prozent der Mails wegen ungültiger Adressen abgefangen – dahinter verbargen sich versuchte Directory-Angriffe auf zuvor mittels Adress-Validierung geschützte Domains.



Zusammenfassung

Die folgende Tabelle zeigt im Detail, welchen Einfluss die Verfahren des Traffic- und Verbindungs-Managements derzeit auf das Aufkommen an unerwünschten E-Mails haben, das MessageLabs misst. Ohne diese zusätzliche Mehr-Ebenen-Abwehr hätte der Anteil von Spam an allen an MessageLabs-Kunden gerichteten E-Mails im September 2007 etwa 85,6 Prozent betragen. Das bedeutet einen Anstieg um 1,9 Prozentpunkte im Vergleich zum Vormonat.

Region	Traffic Management	Verbindungs-Management	Benutzer-Management
USA	47.6%	44.9%	4.2%
GB	49.7%	38.1%	4.2%
Europa	48.2%	38.0%	6.3%
Asien-Pazifik	31.3%	39.9%	0.6%
Weltweit	45.9%	44.9%	4.6%

MessageLabs ist ein führender Anbieter von integrierten Managed Services für die Messaging- und Web-Sicherheit. Bereits mehr als 16.000 Kunden aus 86 Ländern greifen auf die Dienste des Security-Spezialisten zurück – angefangen von Kleinunternehmen bis hin zu Konzernen aus dem Kreis der Fortune 500. Das Portfolio von MessageLabs umfasst eine Vielzahl von verwalteten IT-Sicherheits-Services, um die Kommunikation via E-Mail, Web und Instant Messaging zu schützen, zu kontrollieren, zu verschlüsseln und zu archivieren.

Alle Dienste werden über eine weltweit verteilte Infrastruktur bereitgestellt. Darüber hinaus kommen Kunden in den Genuss eines rund um die Uhr verfügbaren Supports durch ausgewiesene Sicherheitsexperten. Dies gewährleistet einen komfortablen und kosteneffizienten Ansatz, um Risiken durch Online-Gefahren systematisch zu minimieren und beim Austausch von Geschäftsinformationen vor unliebsamen Überraschungen gefeit zu sein. Weitere Informationen finden Sie unter <http://www.messagelabs.com>.

Unter der Internetadresse www.messagelabs.com/intelligence haben Sie zudem die Möglichkeit, sich detailliert über die Leistungen des Geschäftsbereichs MessageLabs Intelligence zu informieren und einen News-Dienst zu abonnieren, der Sie mit aktuellen Alarmmeldungen und Studien versorgt.

Anmerkung: Alle Zahlen in diesem Bericht waren zum Zeitpunkt der Drucklegung korrekt.



Anhang

Anhang I: Spam-Quote nach Ländern

	September	August	Change
Australia	41.3%	36.9%	4.4%
Austria	47.1%	45.0%	2.1%
Belgium	50.0%	51.4%	-1.4%
Canada	57.6%	50.3%	7.3%
China	53.1%	50.4%	2.7%
France	55.5%	58.0%	-2.5%
Germany	48.3%	58.5%	-10.2%
Hong Kong	71.4%	64.8%	6.6%
India	38.1%	32.9%	5.2%
Ireland	54.8%	50.0%	4.8%
Israel	73.8%	70.7%	3.1%
Italy	49.3%	36.7%	12.6%
Japan	27.1%	23.1%	4.0%
Netherlands	36.1%	33.6%	2.5%
Singapore	49.0%	44.0%	5.0%
Spain	42.3%	41.3%	1.0%
Sweden	29.3%	29.5%	-0.2%
Switzerland	47.8%	43.1%	4.7%
United Arab Emirates	39.9%	38.2%	1.7%
United Kingdom	44.5%	41.4%	3.1%
United States	55.5%	50.5%	5.0%



Anhang II: Viren-Quote nach Ländern

	September	August	Change
Australia	0.45%	0.54%	-0.09%
Austria	1.05%	2.20%	-1.15%
Belgium	0.27%	0.51%	-0.24%
Canada	0.53%	1.41%	-0.88%
China	0.86%	1.65%	-0.79%
France	0.78%	1.79%	-1.01%
Germany	0.67%	2.41%	-1.74%
Hong Kong	0.92%	2.15%	-1.23%
India	1.89%	3.60%	-1.71%
Ireland	1.32%	1.28%	0.04%
Israel	0.45%	1.30%	-0.85%
Italy	0.49%	1.83%	-1.34%
Japan	0.41%	0.90%	-0.49%
Netherlands	0.33%	0.13%	0.20%
Singapore	1.03%	2.00%	-0.97%
Spain	0.78%	1.26%	-0.48%
Sweden	0.19%	0.26%	-0.07%
Switzerland	1.08%	2.55%	-1.47%
United Arab Emirates	0.92%	2.38%	-1.46%
United Kingdom	0.90%	1.14%	-0.24%
United States	0.71%	1.18%	-0.47%



Anhang III: Spam-Quote nach Branchen

	September	August	Change
Accom/Catering	45.4%	41.4%	4.0%
Agriculture	67.8%	66.9%	0.9%
Building/Cons	38.4%	31.7%	6.7%
Business Support Services	40.6%	36.7%	3.9%
Chem/Pharm	53.5%	47.8%	5.7%
Education	58.2%	58.1%	0.1%
Estate Agents	35.1%	34.1%	1.0%
Finance	33.8%	30.5%	3.3%
General Services	44.4%	41.7%	2.7%
Gov/Public Sector	40.3%	39.1%	1.2%
Health Care	53.5%	45.7%	7.8%
IT Services	56.0%	49.8%	6.2%
Manufacturing	60.9%	57.0%	3.9%
Marketing/Media	55.0%	53.1%	1.9%
Mineral/Fuel	42.7%	38.0%	4.7%
Non-Profit	47.9%	46.1%	1.8%
Prof Services	49.4%	43.7%	5.7%
Recreation	39.6%	39.2%	0.4%
Retail	49.8%	42.8%	7.0%
Telecoms	67.2%	64.6%	2.6%
Transport/Util	42.8%	40.8%	2.0%
Wholesale	57.7%	51.4%	6.3%



Anhang IV: Viren-Quote nach Branchen

	September	August	Change
Accom/Catering	0.99%	1.57%	-0.58%
Agriculture	0.25%	0.27%	-0.02%
Building/Cons	0.68%	0.82%	-0.14%
Business Support Services	0.46%	0.58%	-0.12%
Chem/Pharm	0.88%	2.16%	-1.28%
Education	2.10%	2.35%	-0.25%
Estate Agents	0.63%	1.09%	-0.46%
Finance	0.62%	0.88%	-0.26%
General Services	0.55%	0.77%	-0.22%
Gov/Public Sector	0.94%	0.97%	-0.03%
Health Care	0.57%	1.06%	-0.49%
IT Services	0.77%	1.33%	-0.56%
Manufacturing	0.75%	1.29%	-0.54%
Marketing/Media	0.88%	1.19%	-0.31%
Mineral/Fuel	0.67%	1.16%	-0.49%
Non-Profit	0.85%	1.05%	-0.20%
Prof Services	0.86%	1.53%	-0.67%
Recreation	0.49%	0.90%	-0.41%
Retail	0.92%	1.72%	-0.80%
Telecoms	0.32%	0.41%	-0.09%
Transport/Util	0.54%	1.01%	-0.47%
Wholesale	1.06%	1.61%	-0.55%