



## MessageLabs Intelligence: August 2009

### *Cutwail erleidet Rückschlag durch ISP-Abschaltung, während Donbot unzähligen Computerbesitzern medizinische Hilfe andient*

Herzlich willkommen zur August-Ausgabe des Monatsberichts von MessageLabs Intelligence. Dieser Report informiert Sie über aktuelle Gefahrentrends im August 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: 88,5 Prozent im August (ein Rückgang um 0,9 Prozentpunkte gegenüber dem Vormonat).*
- *Viren: Eine von 296,6 E-Mails enthielt im August ein Schadprogramm (fast unverändert im Vergleich zum Juli).*
- *Phishing: Hinter einer von 341,2 E-Mails verbarg sich ein Phishing-Angriff (eine Abnahme der Belastung um 0,01 Prozentpunkte seit Juli).*
- *Gefährliche Websites: Pro Tag wurden 3.510 neue Internetseiten gesperrt (ein Minus von 2,9 Prozent gegenüber dem Vormonat).*
- *Abschaltung eines lettischen ISPs bedeutet Rückschlag für Cutwail.*
- *Weitere Spam-Kampagnen setzen auf URL-Abkürzungsdienste.*
- *Social-Networking-Portale von DDoS-Attacken betroffen.*

#### Die Analyse der Ergebnisse

##### Abschaltung eines lettischen ISPs trifft das Botnet Cutwail

Der in der lettischen Hauptstadt Riga ansässige ISP (Internet Service Provider) Real Host war mutmaßlich daran beteiligt, Command-and-Control-Server für infizierte Botnet-Computer sowie Schadprogramm und Phishing-Websites zu betreiben und als Virenfilter getarnte Malware zu verbreiten. Infolgedessen wurde Real Host am 1. August 2009 von den zuständigen Upstream-Providern vom Internet getrennt. Wie Abbildung 1 veranschaulicht waren die Auswirkungen dieser Maßnahme umgehend spürbar: Das Spam-Aufkommen ging in den 48 Stunden nach der Abschaltung kurzzeitig um bis zu 38 Prozent zurück.

Ein erheblicher Teil der offenbar zuvor über Real Host verbreiteten Spam-Mails stand im Zusammenhang mit Cutwail, einem der derzeit größten Botnets, das für rund 15 bis 20 Prozent der gesamten Spam-Belastung verantwortlich ist. Als Real Host vom Netz genommen wurde, ging die Aktivität von Cutwail um bis zu 90 Prozent zurück, jedoch konnte sich das Botnet binnen weniger Tage von diesem Rückschlag wieder erholen.

Abbildung 1 zeigt für den Zeitraum der besagten Maßnahme den relativen Spam-Anteil, der seinen Ursprung in den fünf weltweit größten Botnets nahm: Cutwail, Xarvester, Rustock, Mega-D und Donbot. Die verwendete Messskala ist ein relativer Index, der auf den anteiligen Spam-Mengen und -Quoten beruht, die von den einzelnen Botnets ausgehen. Die Länge der Säulen gibt also nicht direkt Aufschluss über die Größe eines Botnets oder den Umfang der versendeten Spam-Mails. Im nächsten

Intelligence Report wird MessageLabs dann einen genaueren Blick auf einige dieser großen Botnets werfen.

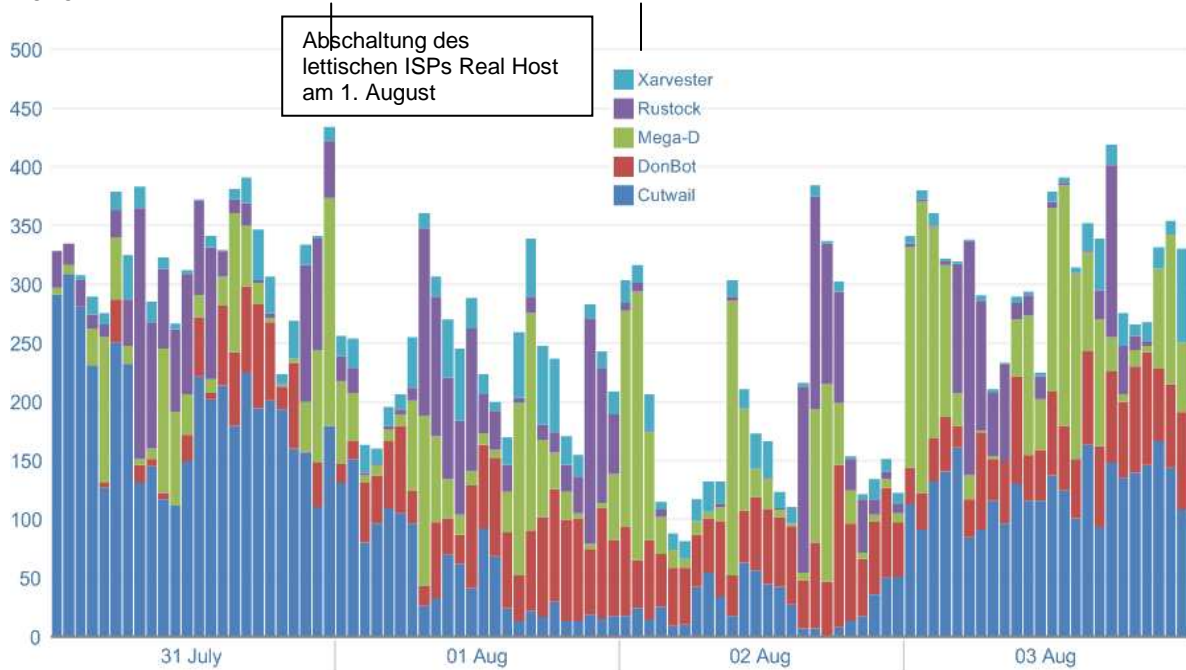


Abbildung 1 – Relativer Spam-Anteil der fünf aktivsten Botnets in dem Zeitraum, in dem Real Host vom Netz genommen wurde

Die Abschaltung von Real Host war nicht der erste Fall, in dem ein ISP unter dem Vorwurf von Viren- und Spam-Aktivitäten vom Netz genommen wurde. In den vergangenen zwölf Monaten widerfuhr mindestens drei in den USA ansässigen ISPs ein ähnliches Schicksal. Dies waren Atrivo (auch als InterCage bekannt), McColo und Pricewert (3FN), wobei die Abschaltung von Pricewert auf Betreiben der Federal Trade Commission der Vereinigten Staaten erfolgte.

### Neue Entwicklungen bei Spam über URL-Abkürzungsdienste

Im Laufe der vergangenen Monate hat MessageLabs Intelligence das steigende Aufkommen von mit Hilfe spezieller Internetdienste abgekürzten Links in Spam-E-Mails verfolgt. Im Internet existiert eine Vielzahl solcher eigentlich seriösen Services, von denen viele permanent von Spammern missbraucht werden. Dies hat solche Ausmaße angenommen, dass einige Anbieter gezwungen waren, ihre URL-Abkürzungsdienste einzustellen. Den Nutzern blieben in diesen Fällen nur zornig formulierte Nachrichten, die sie über die Gründe dieser Maßnahmen in Kenntnis setzten. Die folgenden Abbildungen 2 und 3 zeigen zwei Beispiele solcher Meldungen.

#### Etusivun linkinlyhentäjä.

Etusivun linkinlyhentäjä on toistaiseksi pois käytöstä.

Linkinlyhentäjä tulee jälleen saataville lähiaikoina, kunhan olen ensin lisännyt sisäänkirjautumisvelvoitteen linkkien lyhentämistä varten. Palvelua voivat jatkossa käyttää vain Etusivun viestitalulla keskusteluun osallistuvat käyttäjät, jotka olivat alunperinkin tämän palvelun kohdekäyttäjryhmä.

Huom! OLEN POISTANUT LINKKITIETOKANNAN. Minulla ei ole aikaa erotella satoja Viagran myynti-ilmoituksia sekä porno- ja online-kasino-mainoksia muutamista kunnollisista linkeistä. Valitan Etusivun käyttäjille mahdollisesti koitunutta vaivaa. Viagranmyyjät, olette syvältä!

Please note: the existing link database HAS BEEN PURGED! I don't have the time to sift through the links to separate few valid links from hundreds of Viagra, casino and porn peddlers' links. Viagra sellers, you suck!

Abbildung 2 – Von Spammern missbrauchter URL-Abkürzungsdienst

Qurl.net is currently disabled due to links mostly being made by spamming assholes. Qurl.net is not a spamming service, and better it die than be abused like this.

If you're receiving spam email allegedly From: qurl.net, it isn't sent by me, so stop complaining to me about them; I can't do anything about it.

If you really want them to stop, bug your ISP to enable [SPF](#) (Sender Policy Framework) support, and to reject on SPF FAIL.

And stop replying to spam, you idiots; if you keep doing that, you'll end up getting more!

Abbildung 3 – Wegen Spam-Missbrauch vorübergehend abgeschalteter URL-Abkürzungsdienst

Im Juli und August setzten sich Spam-Kampagnen, die solche Dienste nutzten, mit einer Vielzahl neuer abgekürzter URLs fort. Einen Höhepunkt erreichte die Belastung, wie in Abbildung 4 zu sehen, am 26. Juli mit einem Anteil von 9,25 Prozent am gesamten Spam-Aufkommen. Das entsprach weltweit mehr als 10 Milliarden Nachrichten pro Tag<sup>1</sup>.

Die besagte Spam-Welle warb für pharmazeutische Produkte, und erneut war es das Botnet Donbot, eines der größten derzeit aktiven Netzwerke dieser Art, das sich als Urheber des Angriffs ausmachen ließ.

Hier eine beispielhafte Aufstellung der verwendeten Betreffzeilen:

*Phentermine 37.5 Overnighated to your door*  
*President Obama announced that he's providing affordable meds to people with no health care - Get meds now.*  
*Purchase Meds Online*  
*Obama has OK'd Online Sale of Meds*  
*Zoloft For You*  
*Online Dr. Notes*  
*Obama wants to help YOU get the meds you NEED to be healthy and feel good, get them NOW.*  
*Save 80% on Meds*  
*Obama Opens Online Pharmacy*

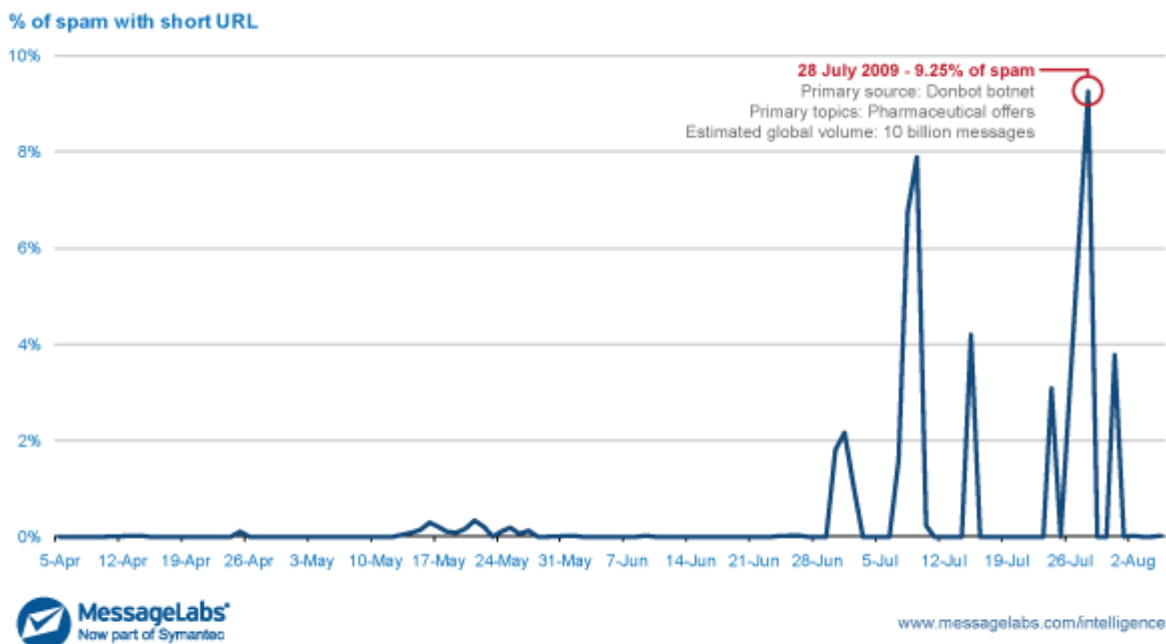


Abbildung 4 – Prozentualer Anteil der Spam-Meldungen, die Links zu URL-Abkürzungsdiensten enthielten

### Spam trägt zu DDoS-Attacken gegen Social-Networking-Seiten bei

Anfang August wurde bekannt, dass eine Reihe sehr bekannter Social-Networking-Portale unter Beschuss von DDoS-Angriffen (Distributed Denial of Service) geraten waren. Diese Attacken standen in Verbindung mit „Joe Job“-Spam, der sich gegen einen russlandfeindlichen Blogger richteten. Beim „Joe Job“-Verfahren handelt es sich um eine Spam-Technik, die bei verschickten E-Mails die Absenderadresse fälscht (d.h. hinter Von: die Adresse eines ahnungslosen Opfers einfügt), sodass

<sup>1</sup> Hochrechnung der weltweiten Spam-Zahlen: [http://www.symantec.com/business/security\\_response/landing/spam/index.jsp](http://www.symantec.com/business/security_response/landing/spam/index.jsp)

Empfänger den Eindruck gewinnen könnten, die Nachricht wäre ihnen von einer realen Person zugesandt worden.

Die erwähnte Spam-Kampagne war, soweit MessageLabs Intelligence dies ermitteln konnte, während dieser Zeit für vermutlich weniger als ein Prozent des gesamten Spam-Aufkommens verantwortlich und wurde über ein bis dato noch nicht klassifiziertes Botnet verbreitet. Die Zahl der verschickten Mails fiel wesentlich geringer aus als bei einigen jüngeren Spam-Attacken, zum Beispiel den von Donbot ausgehenden Kampagnen, die URL-Abkürzungsdienste nutzten.

Auch wenn davon auszugehen ist, dass dieser Spam-Angriff zu den DDoS-Attacken auf Social-Networking-Seiten beigetragen hat, ist es unwahrscheinlich, dass er allein zu den gemeldeten Störungen geführt hat. Das legt die Beteiligung weiterer Akteure nahe. MessageLabs Intelligence vermutet, dass für die DDoS-Attacke synchron auch ein Botnet herangezogen wurde. Dieses dürfte die von ihm kontrollierten Zombie-Rechner befehligt haben, in einem automatischen Prozess jeweils die Website des angegriffenen Social-Networking-Portals zu öffnen.

Abbildung 5 zeigt ein Beispiel für die verschickten Spam-Mails. Die IP-Adresse des Absenders gehört zu einem Rechner in Brasilien, einem Tummelplatz für Botnet-infizierte Computer. Die hinter *From:* angegebene E-Mail-Adresse war gefälscht, um die Empfänger glauben zu lassen, die Nachricht stamme von einem in Ohio ansässigen Unternehmen.

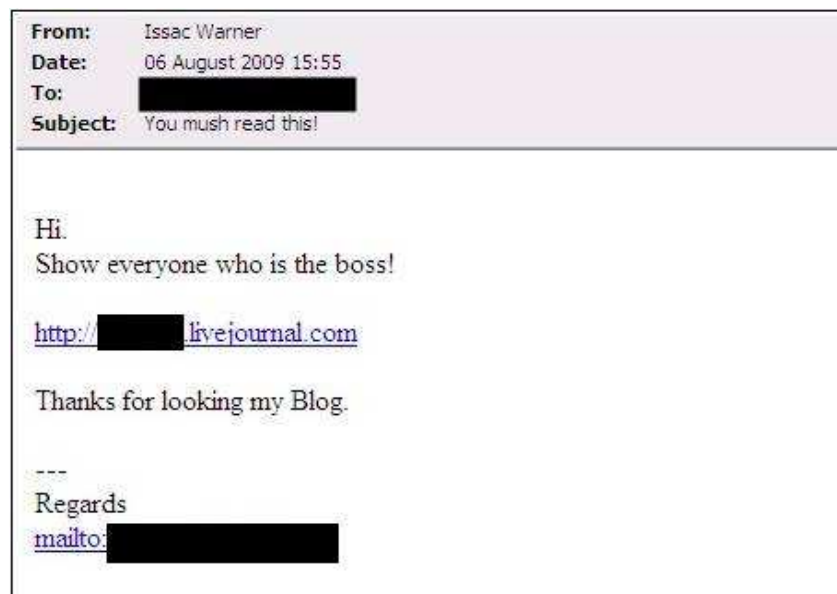


Abbildung 5 - Eine per „Joe Job“-Technik verschickte Spam-Mail, die den Adressaten auffordert, ein bestimmtes Blog zu besuchen

### Der Nutzungszyklus von Web-basierender Malware

Für Online-Betrüger kann es sich als kostspielig erweisen, wenn sie ständig neue Arten von Schadprogrammen entwickeln müssen, um ihre kriminellen Aktivitäten auf auskömmlichem Niveau fortführen zu können. Aus ihrer Sicht ist es weitaus wirtschaftlicher, laufend neue Domains zu registrieren und ihre Malware über so viele Websites und URLs wie möglich zu verteilen, um so jedes neue Schadprogramm länger nutzen zu können. Unter Einsatz serverseitiger Polymorphismen ist es möglich, ein und dieselbe Familie von Virenprogrammen bei jedem Aufruf automatisch und dynamisch auf unterschiedliche Weise in neuen Stämmen zu verpacken. Das macht auf Seiten der Virentfilter permanent neue Signaturen erforderlich, um Schadprogramme zuverlässig zu erkennen. Durch die Kombination solcher Herangehensweisen mit dem Rückgriff auf „schusssichere“ Hosting-Dienste und „Fast-Flux“-Techniken können Internetbetrüger sicherstellen, dass ihre schädlichen Websites nicht immer wieder schnell infolge von Beschwerden vom Netz genommen werden.

In vielen Fällen verfügen organisierte Banden von Online-Kriminellen über hochgrad automatisierte Verfahren, die wenig oder gar keine Aufsicht mehr erfordern. Ihre Systeme sind selbsttätig Tag und Nacht aktiv, um möglichst viele legitime Websites zu manipulieren und neue Domains anzumelden. Sobald diese Abläufe einmal eingerichtet und eingespielt sind, lässt sich eine manipulierte Internetpräsenz je nach verwendeter Angriffsmethode einfach von einem anderen Rechner aus über das Internet neu konfigurieren.

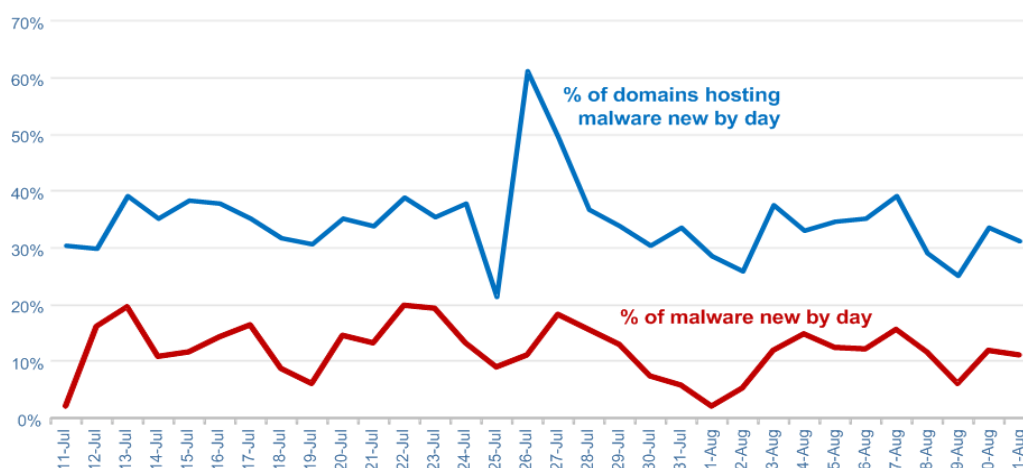


Abbildung 6 – Dieses Kurvendiagramm veranschaulicht wie sich der Anteil neuer Malware und Malware-Websites im Zeitverlauf entwickelt hat.

Die Analysen von MessageLabs Intelligence ergaben für den August, dass pro Tag 3.510 Websites gesperrt werden mussten und dass dies bei durchschnittlich 36,1 Prozent (Anm.: bitte prüfen; der Abbildung nach könnte es auch ein Zahldreher sein – 31,6 %?) dieser Domains zum ersten Mal der Fall war. Abbildung 6 zeigt, wie sich dieser Anteil zuletzt entwickelt hat. In ähnlicher Weise förderte die Untersuchung der auf diese Weise gestoppten Malware zutage, dass es sich pro Tag bei 11,9 Prozent um neue Schadprogrammfamilien gehandelt hat, auf die der Zugriff erstmals unterbunden wurde.

Wenn ein Opfer eine Malware direkt von einer eigentlich seriösen, aber manipulierten Internetseite herunterlädt, wird er unter Umständen erst automatisch über ein komplexes System von Weiterleitungsfunktionen zu dem Server geleitet, über den das Schadprogramm tatsächlich ins Netz gestellt wird. Darüber hinaus stellen Cyberkriminelle oft im Laufe der Zeit immer mehr neue Websites als Sprungbretter zwischen den manipulierten Internetpräsenzen und jenen Endpunkten online, auf denen ihre Malware liegt. Abbildung 7 veranschaulicht dieses Verfahren.

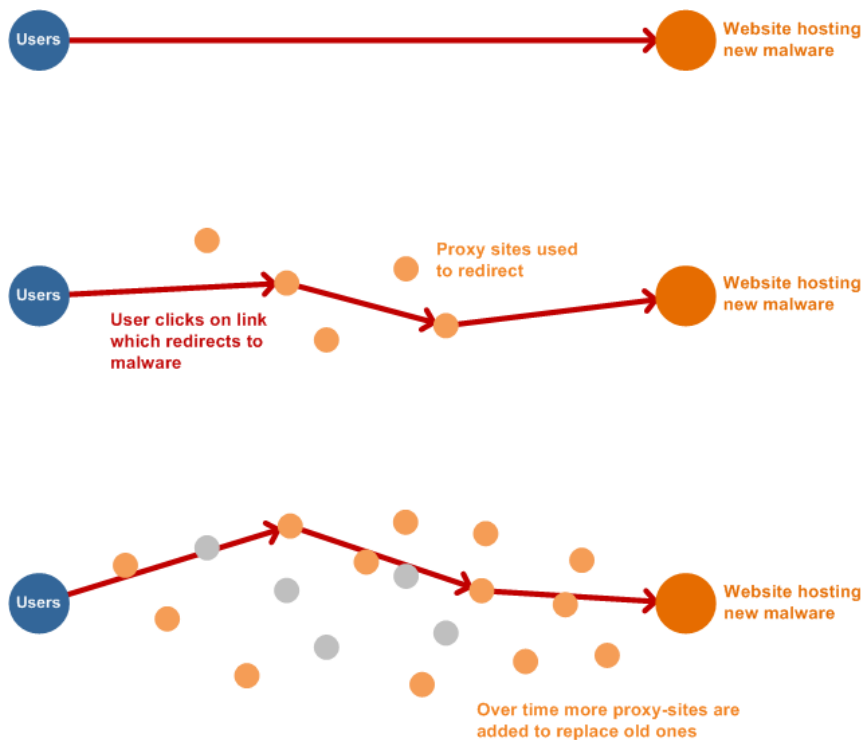


Figure 7 – Diese Grafik zeigt, wie im Laufe der Zeit immer mehr Websites mit einem neuen Schadprogramm verknüpft werden.

Bei dem in Abbildung 7 illustrierten Verfahren wird eine neu entwickelte Art von Schadprogramm zunächst über eine kleine Zahl von Websites ins Netz gestellt oder direkt über andere Internetseiten bzw. über E-Mails verlinkt. Im Laufe der Zeit kommen dann immer mehr Websites ins Spiel, und häufig wird eine simple Weiterleitung genutzt, um Besucher auf eine weitere Sprungbrett-Seite oder unmittelbar zur Malware zu geleiten. Manchmal kommen gleich diverse Weiterleitungen zum Einsatz, die einen Internetnutzer von einer Seite zur nächsten springen lassen, bis dieser schließlich bei dem Virus oder Trojaner angelangt ist. Aus Anwendersicht bleibt dieses Verfahren unsichtbar und ist vielleicht nur dadurch zu erkennen, dass die Ladezeit der Seite länger ausfällt als üblich. Online-Betrüger können über einen solchen Rückgriff auf „Einweg“-Proxy-Server darauf hinwirken, dass die für das Hosting ihrer Malware verwendeten Websites möglichst lange unentdeckt bleiben.

Die Analysen zeigen, dass Tag für Tag weitere seriöse Websites manipuliert und gleichzeitig neue Internetseiten einzig und allein für die Verbreitung von Malware eingerichtet werden. Im August beispielsweise war es so, dass von 100 Domains, die täglich zu sperren waren:

- 36 Domains noch nie zuvor blockiert worden waren.
  - 30 Mal (84,5 Prozent) wurden ältere manipulierte Websites eigentlich seriöser Natur gesperrt.
  - 6 Mal (15,5 Prozent) war der Zugriff auf kürzlich registrierte Domains zu unterbinden.
- 64 Domains auf (seriöse oder sonstige) Web-Adressen entfielen, die schon einmal gesperrt waren oder bereits bekannt sind.

Es ist durchaus üblich, dass Websites mit gewissen Top-Level-Domains (TLDs) nicht in den Ländern betrieben werden, die dem jeweiligen Länderkürzel entsprechen. Dies betrifft zweifellos besonders häufig neu eingerichtete Internetadressen, die für die Verbreitung von Malware eingerichtet werden. Wie Abbildung 8 zeigt, ist bei solchen Websites die Wahrscheinlichkeit signifikant größer, dass der eigentliche Server-Standort nicht mit der Top-Level-Domain übereinstimmt.

In die Tabelle wurden auch die nicht an einzelne Länder geknüpften TLDs aufgenommen, um die Standorte der mit ihnen betriebenen Malware-Websites aufzuzeigen.

### Hosting Locations For Most Frequent Top-Level Domains Blocked

	Top-Level Domain						
	.cn	.in	.ru	.us	.com	.info	.net
Canada					18.8%	61.6%	11.0%
Cayman Islands					10.1%		
China	46.0%	33.3%	18.2%	3.2%	7.2%	1.2%	8.7%
Estonia			4.5%				
France		4.8%					
Germany				3.2%	6.4%		
Hong Kong							1.0%
Ireland	17.0%						
Latvia			22.7%		2.4%		1.0%
Luxembourg						2.0%	2.2%
Namibia	2.4%						
Netherlands					2.9%	5.0%	2.0%
Panama		22.0%					
Poland		4.8%			2.1%		3.0%
Romania							9.0%
Russia	7.1%	7.0%	40.9%		4.0%		18.0%
Serbia					10.1%		
Singapore							3.0%
Taiwan	4.0%						
Ukraine	23.0%				6.9%		15.0%
United Kingdom			9.1%				
United States		28.0%	4.5%	93.5%	20.4%	30.0%	22.0%

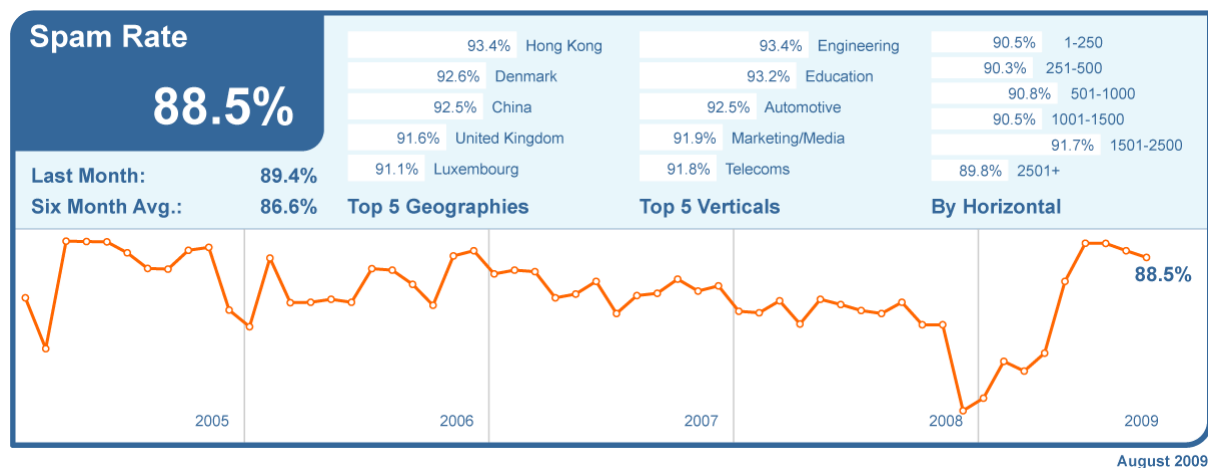
Abbildung 8 – Die am häufigsten für das Hosting von gefährlichen Website-Inhalten genutzten Top Level Domains (nach Server-Standorten).

Bei schon länger existierenden, seriösen Websites, die für die Malware-Verbreitung manipuliert worden sind, sieht das Bild anders. Hier stimmt die Top-Level-Domain wesentlich häufiger mit dem zu erwartenden Server-Standort überein.

## 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 unbekanntem zweifelhaften Quellen stammen und an gültige E-Mail-Adressen gerichtet sind.

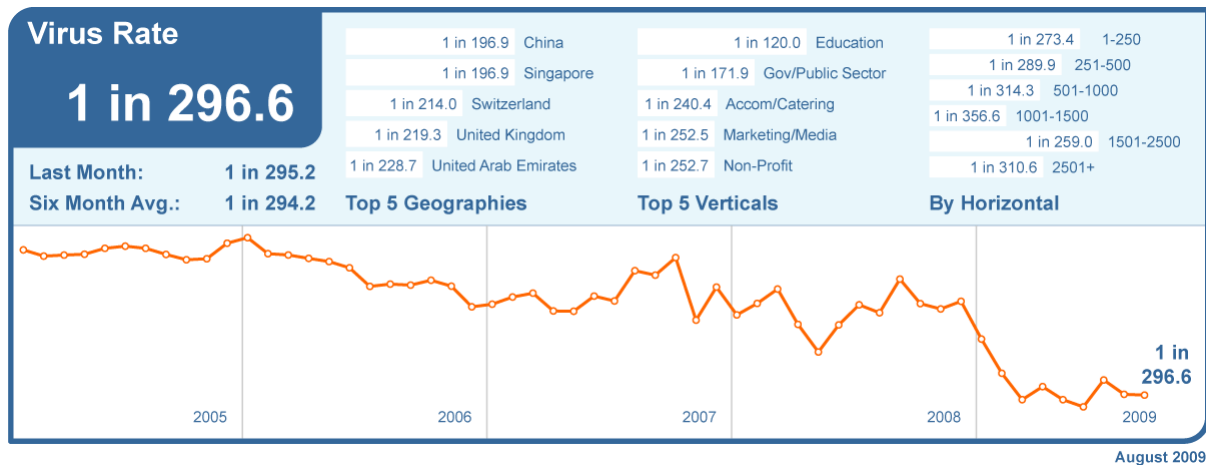
**Spam-Schutz mit Skeptic™:** Im August 2009 belief sich der weltweite Anteil von Spam-Nachrichten am E-Mail-Verkehr aus neuen oder bisher nicht als böse bekannten Quellen auf 88,5 Prozent (oder eine von 1,13 E-Mails). Das bedeutet einen Rückgang um 0,9 Prozentpunkte gegenüber Juli.



Trotz eines Rückgangs der Spam-Quote um 0,8 Prozentpunkte auf nunmehr 93,4 Prozent belegte Hongkong im August die Spitzenposition als das Land, das weltweit am meisten unter Spam zu leiden hat. In den USA stieg die Spam-Quote auf 89,5 Prozent und in Kanada auf 88,7 Prozent. Die meisten anderen Länder erlebten derweil eine rückläufige Belastung mit unerwünschten Werbe-Mails. In Großbritannien sank der Anteil von Spam-Nachrichten am E-Mail-Verkehr auf 91,6 Prozent, in Deutschland auf 90,4 Prozent, in Frankreich auf 90,7 Prozent und in den Niederlanden auf 86,3 Prozent. In Australien ging die Spam-Quote auf 90,6 Prozent zurück, in Japan auf 89,2 Prozent.

**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 August auf 1 zu 296,6 (bzw. 0,34 Prozent) und war damit gegenüber dem Vormonat weitgehend unverändert.

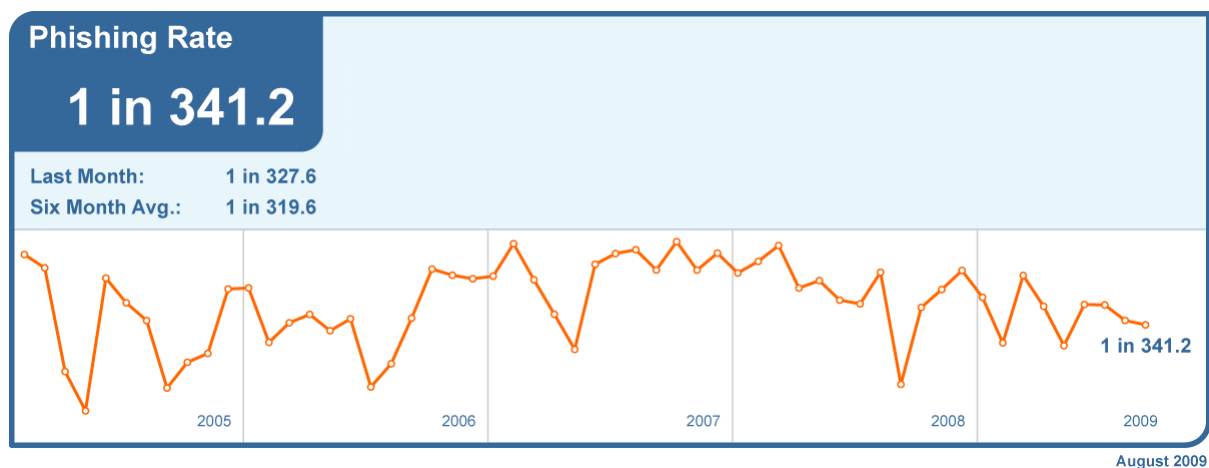
Ein Anteil von 14,8 Prozent der via E-Mail verbreiteten Malware beruhte im August auf Links zu gefährlichen Websites. Das waren 0,4 Prozentpunkte weniger als noch im Juli. Als vermeintliche Online-Postkarten getarnte Mails waren im August für 21,3 Prozent dieser gefährlichen Links verantwortlich.



In Chinaging der Anteil schadprogrammverseuchter E-Mails im August zwar auf 1 zu 196,9 zurück, dennoch belegte das Land den ersten Platz im weltweiten Viren-Ranking. Singapur und die Schweiz verteidigten mit Viren-Quoten von 1 zu 196,9 (Anm.: bitte prüfen; derselbe Wert wie China?) bzw. 1 zu 214,0 ihre Position unter den fünf am stärksten betroffenen Ländern. Komplettiert wurde die Top 5 des Viren-Rankings im August von Großbritannien mit einer Quote von 1 zu 219,3 und den Vereinigten Arabischen Emiraten, wo der Anteil schadprogrammverseuchter E-Mails 1 zu 228,7 betrug.

Deutschland und die Niederlande hatten mit Viren-Quoten von 1 zu 275,5 bzw. 1 zu 612,18 eine steigende Belastung mit verseuchten E-Mails zu verzeichnen. In den Vereinigten Staaten ging der Anteil virenbelasteter Mails leicht auf 1 zu 387,1 zurück, während dieser in Kanada auf 1 zu 309,9 zulegte. Australien, das im Juli noch das am stärksten betroffene Land gewesen war, fand sich im August mit einer Quote von 1 zu 308,3 auf Platz 12 im weltweiten Viren-Ranking wieder. Für Hongkong konnte MessageLabs Intelligence einen Anteil verseuchter E-Mails von 1 zu 297,7 ermitteln und für Japan von 1 zu 400,76.

**Phishing:** Der August brachte im Vergleich zum Vormonat einen Rückgang der Phishing-Quote um 0,01 Prozentpunkte. Bei einer von 341,2 E-Mails (bzw. 0,29 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 sank der Anteil von Phishing-Nachrichten im Juli um 6,0 Prozentpunkte auf 86,9 Prozent.



**Skeptic™ Web Security Services Version 2.0:** Die Website-Kategorie „Werbung & Popups“ war im August mit einem Anteil von 58,03 Prozent der häufigste Auslöser von regel- und richtliniengesteuerten Filterungsaktivitäten, die im Rahmen des Dienstes MessageLabs Web Security für Geschäftskunden erfolgt sind. Gegenüber Juli bedeutet dies einen Rückgang um 2,07 Prozentpunkte.

Die Analyse der von diesem Web-Sicherheits-Service getroffenen Maßnahmen zeigt, dass es sich im August bei 45,4 Prozent aller abgefangenen, über das Internet verbreiteten Schadprogramme um neue Angriffe gehandelt hat. Im Vergleich zum Vortag ergibt sich daraus eine Steigerung um 44,7 Prozentpunkte. Bei Web-basierender Spyware ging der Anteil neuer Varianten im August um 0,01 Prozentpunkte auf 19,5 Prozent zurück.

Durchschnittlich hat MessageLabs Intelligence im August pro Tag 3.510 Internetseiten aufgespürt, auf denen Malware und andere möglicherweise unerwünschte Programme wie etwa Spyware und Adware hinterlegt waren. Das waren 2,9 Prozent weniger als noch im Juli.

**Web Security Services (Version 2.0) Activity:**

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	58.03%	Infostealer.Gampass	7.90%	PUP:WebToolbar.Win32.MyWebSea...	56.13%
Streaming Media	11.76%	New Unclassified Trojan	3.46%	PUP:WebToolbar.Win32.Zango.ca	5.36%
Downloads	5.04%	Suspicious.Graybird.1	3.20%	PUP:ZangoSearch	3.36%
Games	4.54%	New Unclassified VirusVirus	3.06%	PUP:PSWTool.Win32.WinPassViewer.q	1.54%
Peer-to-Peer	2.39%	Trojan.Fakevalert	2.59%	PUP:RiskTool.VBS.DisReg.a	1.45%
Chat	2.12%	Infostealer.Bancos	2.34%	PUP:NetTool.Win32.Portscan.c	1.45%
Blogs & Forums	2.04%	Trojan-Downloader.JS.Iframe.aqu	2.27%	PUP:Client-IRC.Win32.mIRC.g	1.36%
Adult/Sexually Explicit	1.93%	Packed.Generic.233	1.63%	PUP:PUP:Win32.BHO.gtq	0.91%
Computing & Internet	1.49%	Suspicious.MH690	1.45%	PUP:BetterInternet	0.91%
Personals & Dating	1.49%	Bloodhound.DirActCOM	2.14%	PUP:Win32.Shopper.v	0.82%

August 2009

Das folgende Kurvendiagramm veranschaulicht, wie sich im August das Aufkommen an täglich neu zu sperrenden Viren- und Trojaner-Seiten im Vergleich zur entsprechende Zahl der pro Tag blockierten Websites mit Spyware und Adware entwickelt hat.

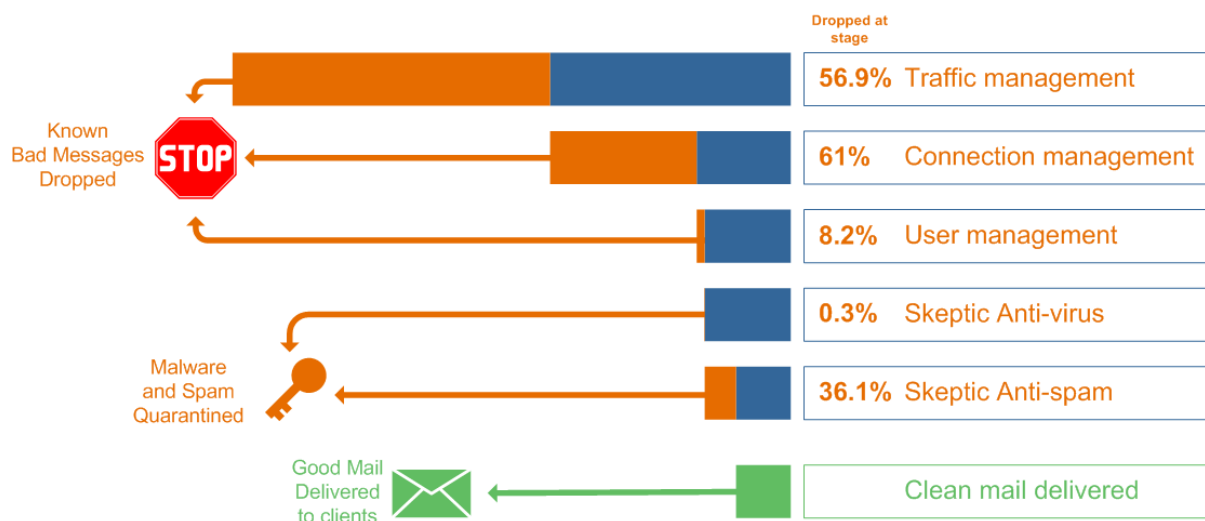


August 2009

## 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 August wurden im Rahmen der MessageLabs-Dienste durchschnittlich 3,95 Milliarden SMTP-Verbindungen pro Tag verarbeitet. Davon wurden 56,9 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-Angriffe 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 August wurden auf diese Weise durchschnittlich 61,0 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 August wurden durchschnittlich 8,2 Prozent der eingehenden Mails wegen ungültiger Adressen abgefangen. Dahinter verbargen sich versuchte Directory-Angriffe 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 21.000 Kunden aus 99 Ländern überprüfen. Weiterführende Informationen finden sich im Internet unter [www.messagelabs.com/intelligence](http://www.messagelabs.com/intelligence).

### **Über Symantec**

Symantec ist ein weltweit führender Anbieter von Infrastruktur-Software, mit der sich Unternehmen und Privatpersonen sicher und vertrauensvoll in einer vernetzten 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](http://www.symantec.de).

Copyright © 2009 Symantec Corporation. Alle Rechte vorbehalten.

Symantec, das Symantec-Logo und MessageLabs sind Schutzmarken oder eingetragene Warenzeichen der Symantec Corporation oder ihrer Partner in den USA und in anderen Ländern. Bei weiteren Produkt- und Firmennamen handelt es sich möglicherweise um Warenzeichen ihrer jeweiligen Besitzer.

OHNE GEWÄHR. Die in diesem Dokument enthaltenen Informationen werden ohne jegliche Gewährleistung bereitgestellt. Die Symantec Corporation übernimmt keinerlei Garantie hinsichtlich deren Richtigkeit und Verwendung. Wer in diesem Dokument enthaltene Informationen gebraucht, trägt dafür allein alle Risiken. Unter Umständen kann dieser Bericht technische und sonstige Ungenauigkeiten oder Tipp- bzw. Druckfehler enthalten. Symantec behält sich das Recht vor, Informationen ohne vorherige Ankündigung zu ändern. Kein Teil dieser Veröffentlichung darf ohne ausdrückliche schriftliche Genehmigung durch die Symantec Corporation (20330 Stevens Creek Blvd., Cupertino, CA 95014, USA) vervielfältigt werden.