MessageLabs Intelligence: April 2009

Grafik-Spam feiert Renaissance und lässt die Spam-Quote auf ein 19-Monats-Hoch von mehr als 85 Prozent steigen

Herzlich willkommen zur April-Ausgabe des Monatsberichts von MessageLabs Intelligence. Dieser Report informiert Sie über aktuelle Gefahrentrends im April 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: 85,3 Prozent im April (ein Anstieg um 9,6 Prozentpunkte gegenüber März).*
- *Viren: Eine von 304,9 E-Mails enthielt im April ein Schadprogramm (ein Minus von 0,08 Prozentpunkten im Vergleich zum Vormonat).*
- *Phishing: Hinter einer von 404,7 E-Mails verbarg sich ein Phishing-Angriff (ein Rückgang um 0,10 Prozentpunkte seit März).*
- *Gefährliche Websites: Pro Tag wurden 3.561 neue Internetseiten gesperrt (eine Steigerung um 27,3 Prozent gegenüber März).*
- *Grafik-Spam über Website-Weiterleitungen auf dem Vormarsch: Spammer „entführen" seriöse Domains, um von deren gutem Ruf zu profitieren.*
- *G-20-Gipfel provoziert gezielte Angriffe gegen Finanzinstitute.*
- *„Aprilscherze" von Downadup (alias Conficker).*

Die Analyse der Ergebnisse

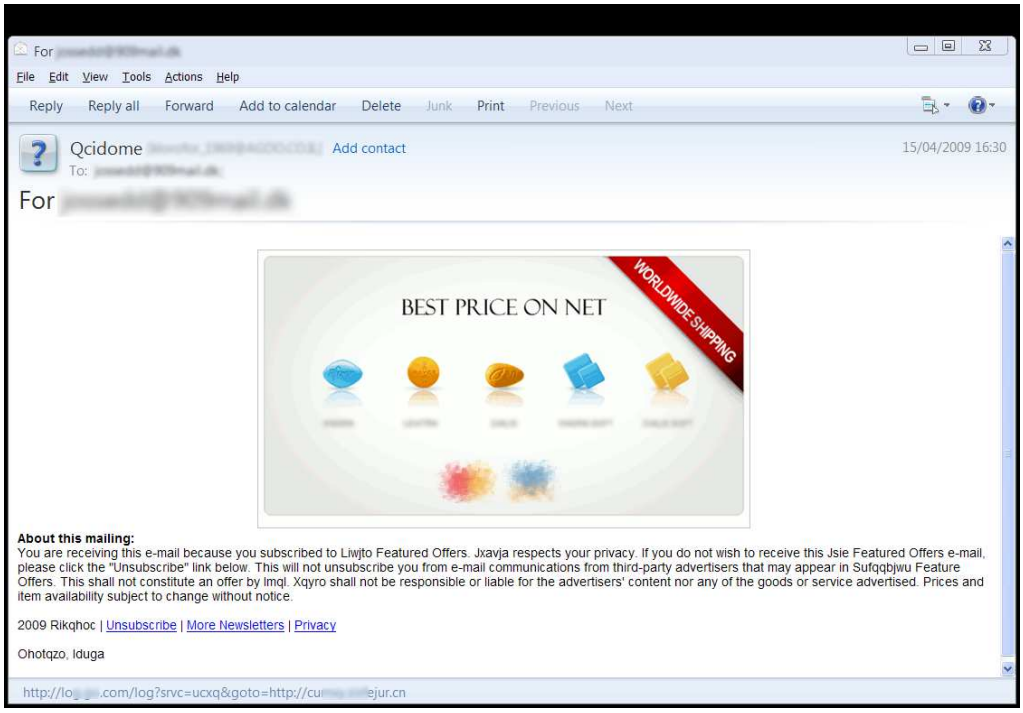
Grafik-Spam gibt ein unwillkommenes Comeback und hebt die Spam-Quote unter Rückgriff auf Website-Weiterleitungen zum ersten Mal seit September 2007 über die 85-Prozent-Marke

Die Erhebungen von MessageLabs Intelligence haben ergeben, dass der Anteil von Spam-Nachrichten am E-Mail-Verkehr zum ersten Mal seit 19 Monaten über die 85-Prozent-Marke geklettert ist. Grafik-Spam war ein Phänomen, das seinen Höhepunkt im Jahr 2007 erlebt hat. Zu dieser Zeit ging es dabei um E-Mails mit angehängten Dateien beispielsweise im gif- oder jpg-Format, in die Spam-Inhalte eingebettet waren. Häufig enthielten die auf diesem Wege verbreiteten Bilddateien einen Text, der als Grafik aufbereitet wurde, um auf diese Weise herkömmliche Spam-Filter zu umgehen, die den Textteil von E-Mails auf verdächtige Wortmuster hin untersuchen.

Betrachtet man indes die Gegenwart, erlebt man eine ganz andere Vorgehensweise: Mittlerweile stellen Spammer derartige Bilddateien über eigentlich vertrauenswürdige Hosting-Seiten ins Netz und vertrauen zugleich auf die Weiterleitung über andere seriöse Websites, um so den wahren Speicherort der Grafiken zu verschleiern. Mit dieser Technik hoffen sie, Filter zu umgehen, die bei der Prüfung von E-Mails auch die Internetadressen der enthaltenen Links untersuchen. Viele Tools zur Spam-Abwehr nutzen derartige Verfahren, um das Wesen solcher Domains einzuschätzen und daraufhin Rückschlüsse auf die Wahrscheinlichkeit ziehen zu können, mit der es sich bei einer E-Mail um eine Spam-Nachricht handelt.

Das folgende Beispiel veranschaulicht, dass die verschickten Spam-Mails auch Standard-Textbausteine enthalten, die darauf abzielen, dass die Nachrichten seriös wirken und im Einklang mit Anti-Spam-Gesetzen wie dem „Can-Spam Act“ in den Vereinigten Staaten zu stehen scheinen. Dazu gehören beispielsweise Hinweise auf die Möglichkeit, sich aus einem E-Mail-Verteiler auszutragen, und Links zu Datenschutzbestimmungen.

Zudem enthält diese Mail in ihrem Textteil auch randomisierte Wörter, um auf diese Weise Fingerprinting-Filter zu umschiffen.

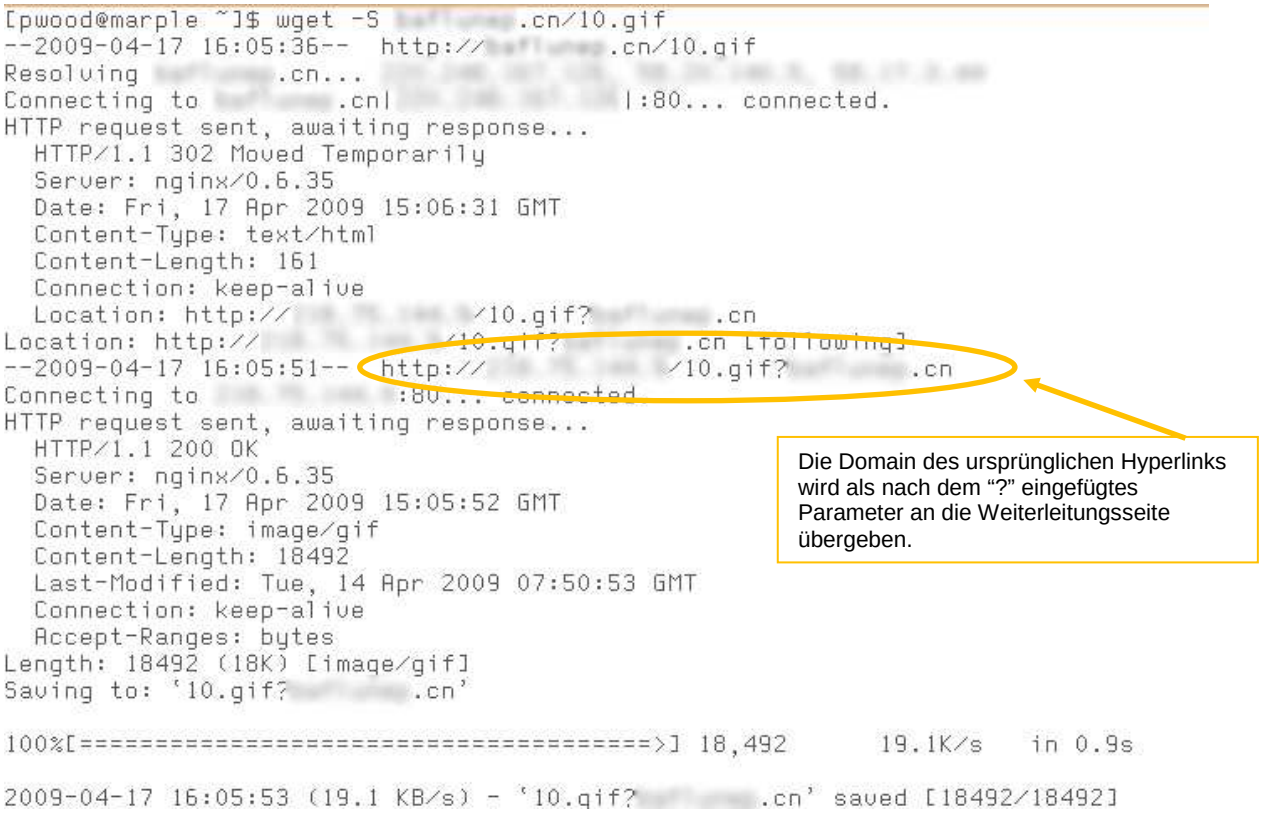


Im oben dargestellten Beispiel findet sich in der E-Mail die folgende URL, damit innerhalb der Nachricht die Spam-Grafik dargestellt wird:

```
<img src="http://[redux].com/log?srvc=xmibx&goto=http://[redux].cn/10.gif"
border=0 alt="Qbjwjvuda Click Here!">
```

Dieser Weiterleitungs-Link lässt sich zu einer weiteren Website zurückverfolgen, die ihrerseits – wie im Folgenden zu sehen ist – ebenfalls vom Web-Server weitergeleitet wird, bevor die angefragte Grafik endlich abgerufen wird. Zu beachten ist, dass der Domain-Name des ursprünglichen Hyperlinks beim Download der Datei bewahrt und als Parameter der URL übergeben wird, zum Beispiel in dieser Form: `http://[weitergeleitete IP-Adresse]/10.gif?[ursprüngliche Domain]`

Anzunehmen ist, dass Spammer dieses Verfahren verwenden, um die tatsächliche Nutzung jeder einzelnen Domain verfolgen zu können. Möglicherweise geht es ihnen dabei darum, deren Langlebigkeit und Effektivität im Zeitablauf zu erfassen.



Zu den weiteren Beispielen für solche Verschleierungsversuche gehörten auch Spam-Nachrichten, die darauf ausgerichtet sind, sich Spamfiltern unter Rückgriff auf HTML-Style-Tags zu entziehen. Solche Tags dienen dazu, randomisierte Texte zu verbergen und Spam-Filter auf diese Weise zu irritieren. Das sieht zum Beispiel wie folgt aus:

```
<STYLE>Ysavu ujkuibito Yna wuc</STYLE>
```

Der Text zwischen den Style-Tags wird in der E-Mail-Nachricht nicht angezeigt und bleibt unsichtbar, jedoch lassen sich einige herkömmliche Spam-Filter der naiven Art bereits durch den Einsatz einer derart simplen Maßnahme aus dem Konzept bringen. Verwendung hat das Verfahren auch gefunden, um die Domains der verlinkten Seiten aufzuspalten, wie es das folgende Beispiel veranschaulicht:

```
www.spammerdomain<STYLE>Zowjqs otuwaqito Fodi ahqwu</STYLE>name.cn
```

Auch in diesem Fall wird der Text zwischen den HTML-Style-Tags nicht angezeigt. Jedoch gibt es einige Tools zur Spam-Abwehr, bei denen es zu Verwechslungen kommen kann, weil sie vor der Analyse einer solchen Mail einfach die Style-Tags entfernen. Im gezeigten Beispiel würden sie demnach davon ausgehen, dass die Internetadresse `ahqwh.name.cn` lauten würde.

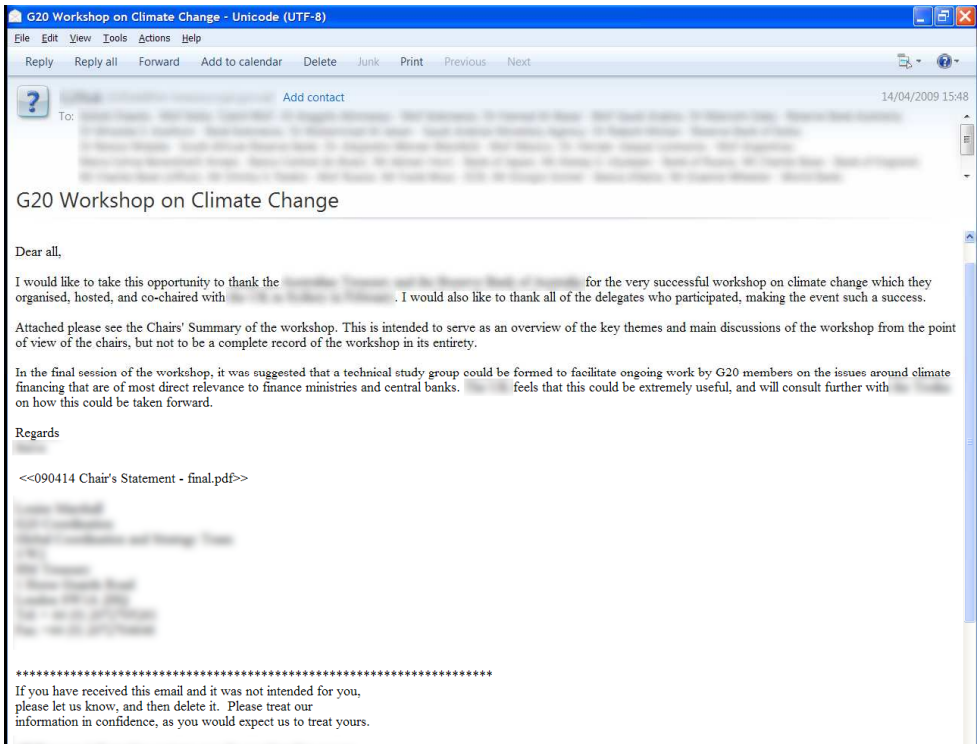
Außerdem enden viele der Top-Level-Domains, über die Spammer ihre Bilder ins Netz stellen, mit dem Länderkürzel „.cn“ für China. Das mag darauf zurückzuführen sein, dass die meisten Partner der wichtigen TLD-Registrierungsstellen im Hinblick auf die Anmeldung und Freischaltung von Spam-Seiten mittlerweile wesentlich vorsichtiger zu Werke gehen, was die Registrierung solcher Domains erheblich erschwert. Infolgedessen sind Spammer gezwungen, Internetadressen in Ländern in Übersee zu registrieren, wo die zuständigen Registrierungsstellen die Anträge offensichtlich nicht so streng prüfen.

Der jüngste G-20-Gipfel in London war der Aufhänger einer Reihe gezielter Trojaner-Angriffe im März und April

Am 2. April 2009 kamen die Finanzminister und Zentralbankchefs der zwanzig wichtigsten Industrie- und Schwellenländer (G-20) in London zusammen. Das Treffen fand nicht nur ein enormes internationales Medieninteresse, sondern löste auch eine schwunghafte Zunahme gezielter Malware-Attacken in den vergangenen zwei Monaten aus.

Hatte sich die pro Tag im Durchschnitt gemessene Zahl solcher Angriffe im Jahr 2008 noch auf 53 belaufen, so stieg sie schon im ersten Quartal 2009 auf 60. Im Vorfeld und in den Tagen nach dem G20-Gipfel am 2. April in London legte die Bedrohung sogar auf rund 100 tägliche Attacken zu, bevor sie dann wieder auf rund 60 pro Tag zurückging.

Zu den Adressaten dieser Attacken zählten auch einzelne Mitarbeiter der an den G-20-Treffen beteiligten Zentralbanken. Die folgende Abbildung zeigt ein Beispiel für die verschickten E-Mails:


G20 Workshop on Climate Change - Unicode (UTF-8)

File Edit View Tools Actions Help

Reply Reply all Forward Add to calendar Delete Junk Print Previous Next

Add contact 14/04/2009 15:48

To:

G20 Workshop on Climate Change

Dear all,

I would like to take this opportunity to thank the for the very successful workshop on climate change which they organised, hosted, and co-chaired with . I would also like to thank all of the delegates who participated, making the event such a success.

Attached please see the Chairs' Summary of the workshop. This is intended to serve as an overview of the key themes and main discussions of the workshop from the point of view of the chairs, but not to be a complete record of the workshop in its entirety.

In the final session of the workshop, it was suggested that a technical study group could be formed to facilitate ongoing work by G20 members on the issues around climate financing that are of most direct relevance to finance ministries and central banks. feels that this could be extremely useful, and will consult further with on how this could be taken forward.

Regards

<<090414 Chair's Statement - final.pdf>>

****

If you have received this email and it was not intended for you, please let us know, and then delete it. Please treat our information in confidence, as you would expect us to treat yours.

Die E-Mails enthielten jeweils einen Anhang im PDF-Format. Sobald jemand dieses Dokument öffnete, wurde auf dem betreffenden Rechner ein Trojaner-Downloader installiert und ausgeführt. Dieses Schadprogramm wiederum lud dann weitere Spyware-Komponenten auf den Zielcomputer herunter.

Begonnen haben diese gezielten Attacken schon Anfang Februar und Anfang März, als der anstehende G-20-Gipfel bei Techniken des Social Engineerings als thematischer Aufhänger diente. Anschließend intensivierten sich in der Zeit bis Anfang April die Angriffe gegen Finanzinstitute und Zentralbanken. Die Phase der größten Bedrohung begann ungefähr Mitte März im Vorfeld eines G-20-Vortreffens wichtiger Akteure aus der Finanzwelt. Auffällig war, dass man einige der für gezielte Attacken verschickten Nachrichten als Antworten auf reale, aber harmlose E-Mails gestaltet hatte. Das legt den Schluss nahe, dass der Rechner mindestens eines Empfängers bereits zuvor infiziert war.

Viren und ihre „Aprilscherze“: Downadup (alias Conficker oder Kido) aktualisiert sich am 1. April

Der 1. April ist rund um den Erdball traditionell der Tag des Jahres, an dem sich die Menschen gegenseitig hereinlegen. In diesem Jahr war das Datum jedoch noch aus einem anderen Grund von Belang, wurde es doch in Zusammenhang mit dem jüngsten Ausbruch der Malware Downadup gebracht. Sicherheitsexperten hatten nämlich herausgefunden, dass bereits mit einem früheren Stamm dieses Virus infizierte Rechner so manipuliert werden können, dass sie am 1. April automatisch ein Update auf die neuere, ausgereiftere Version Dowadup.C vornehmen.

Dieses Update erweitert das Schadprogramm um weitere Funktionen, mit deren Hilfe es sich einer Erkennung und möglichen Störungen besser entziehen kann. Darüber hinaus bringt die aktuelle Version der Malware auch erstmals neue Gegenmaßnahmen gegen Virenscanner zum Einsatz, mit der sie bestimmte Prozesse abbricht, die von einigen Abwehr-Tools genutzt werden.

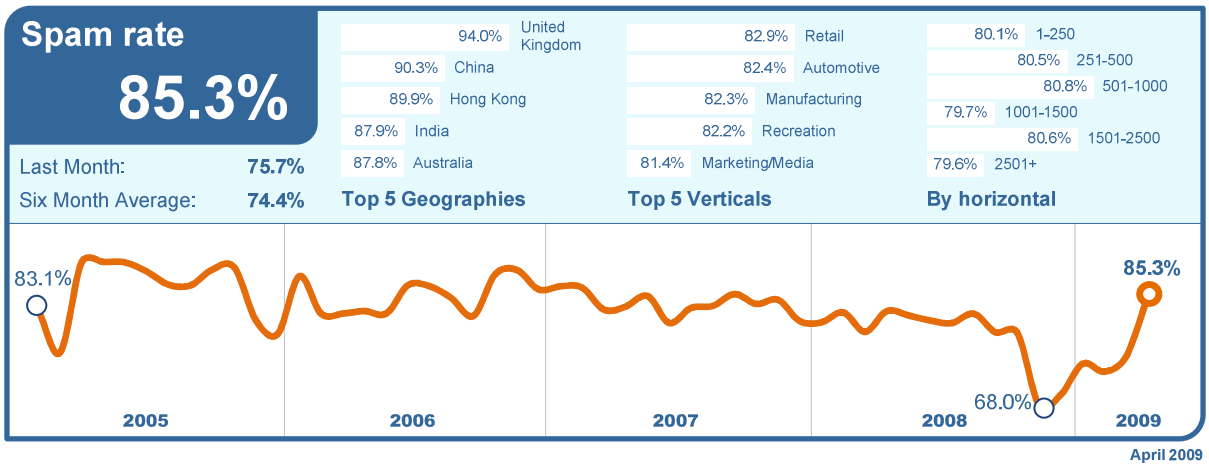
Am 8. April wurde mit Downadup.E ein neuer Stamm des Schadprogramms aufgespürt, der scheinbar auch den Waledac-Virus auf den betroffenen Rechnern installiert.

Weiterführende Informationen zum Downadup-Virus und Hinweise, wie sich Computerbesitzer mit einigen simplen Maßnahmen wirksam schützen können, finden sich auf der Symantec-Website unter: http://service1.symantec.com/SUPPORT/ent-security.nsf/docid/2009033012483648

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 April 2009 belief sich weltweit der Anteil von Spam-Nachrichten am E-Mail-Verkehr aus neuen oder bisher nicht als bösartig bekannten Quellen auf 85,3 Prozent (oder eine von 1,17 E-Mails). Das bedeutet eine Zunahme um 9,6 Prozentpunkte gegenüber März.



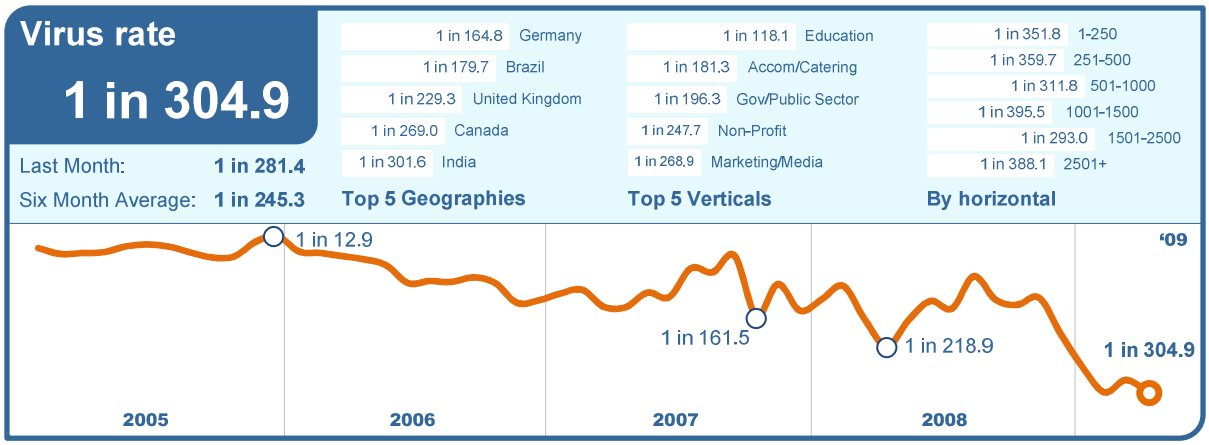
April 2009

Mit einem Anstieg der Spam-Quote um 25,6 Prozentpunkte auf nunmehr 94,0 Prozent war Großbritannien im April das Land, das weltweit unter der höchsten Spam-Belastung zu leiden hatte. In den USA legte die Spam-Quote auf 79,4 Prozent zu, in Kanada belief sie sich auf 77,4 Prozent und in Hongkong auf 89,9 Prozent. In Deutschland erreichte sie einen Wert von 83,3 Prozent und in den Niederlanden von 78,0 Prozent. In Australien entfielen 87,8 Prozent des E-Mail-Verkehrs auf Spam, in China waren es 90,3 Prozent und in Japan 86,4 Prozent.

Mit einer Spam-Quote von 82,9 Prozent stand der Einzelhandel im April stärker unter Beschuss von Spam-Mails als jede andere Branche. Der Bildungssektor erreichte eine Spam-Quote von 81,1 Prozent und die Chemie- und Pharma-Industrie von 77,3 Prozent. Bei Behörden belief sich dieser Wert auf 76,1 Prozent und in der Finanzindustrie auf 78,2 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 April auf 1 zu 304,9 (bzw. 0,28 Prozent). Das ist ein Rückgang um 0,08 Prozentpunkte gegenüber dem Vormonat.

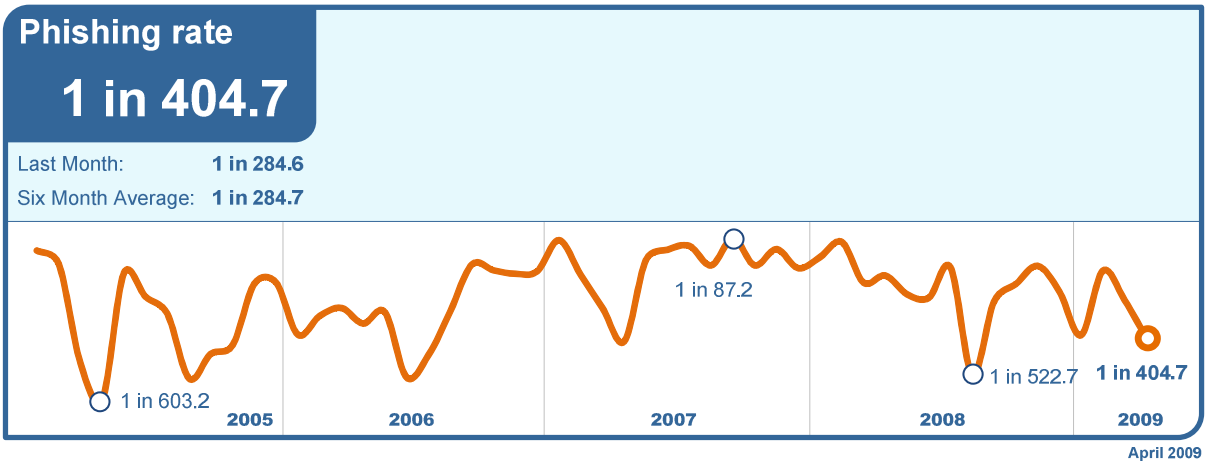
Ein Anteil von 13,3 Prozent der mittels E-Mail verbreiteten Malware beruhte auf Links zu gefährlichen Websites. Das sind 6,9 Prozentpunkte weniger als noch im März. Als vermeintliche Online-Postkarten getarnte Mails waren im April für 61,5 Prozent dieser gefährlichen Links verantwortlich, wobei weitere 8,6 Prozent in Verbindung mit den Botnets Storm oder Waledac standen.



In Deutschland stieg der Anteil schadprogrammverseuchter E-Mails im April um 0,07 Prozentpunkte auf 1 zu 164,8. 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 512,1, in Kanada waren es 1 zu 269,0 und in Australien 1 zu 908,8. In Großbritannien belief sich das entsprechende Verhältnis auf 1 zu 229,3, in China auf 1 zu 338,1, in Hongkong auf 1 zu 370,8 und in Japan auf 1 zu 1883,2.

Der Bildungssektor verteidigte im April trotz einer um 0,19 Prozentpunkte auf einen Anteil von nunmehr 1 zu 118,1 E-Mails gesunkenen Viren-Quote seinen ersten Platz im Ranking der Branchen, die sich mit dem höchsten Prozentsatz verseuchter E-Mails konfrontiert sahen. Bei IT-Dienstleistern belief sich die Viren-Quote auf 1 zu 367,3, bei Einzelhandelsunternehmen auf 1 zu 506,1 und bei Finanzdienstleistern auf 1 zu 446,9.

Phishing: Der April brachte im Vergleich zum März einen Rückgang der Phishing-Quote um 0,10 Prozentpunkte. Bei einer von 404,7 E-Mails (bzw. 0,25 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 April um 9,2 Prozentpunkte auf 89,7 Prozent.



Skeptic™ Web Security Services Version 2.0: Die Website-Kategorie „Werbung & Popups“ war im April 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 März bedeutet dies eine Zunahme um 21,6 Prozentpunkte.

Die Analyse der von diesem Dienst zur Web-Sicherheit getroffenen Maßnahmen zeigt, dass es sich im April bei 63,3 Prozent aller abgefangenen, über das Internet verbreiteten Schadprogramme um neue Angriffe gehandelt hat. Im Durchschnitt hat MessageLabs Intelligence pro Tag 3.561 neue Seiten aufgespürt, auf denen Malware und andere möglicherweise unerwünschte Programme wie etwa Spy- und Adware hinterlegt waren. Das waren 27,3 Prozent mehr als noch im März.

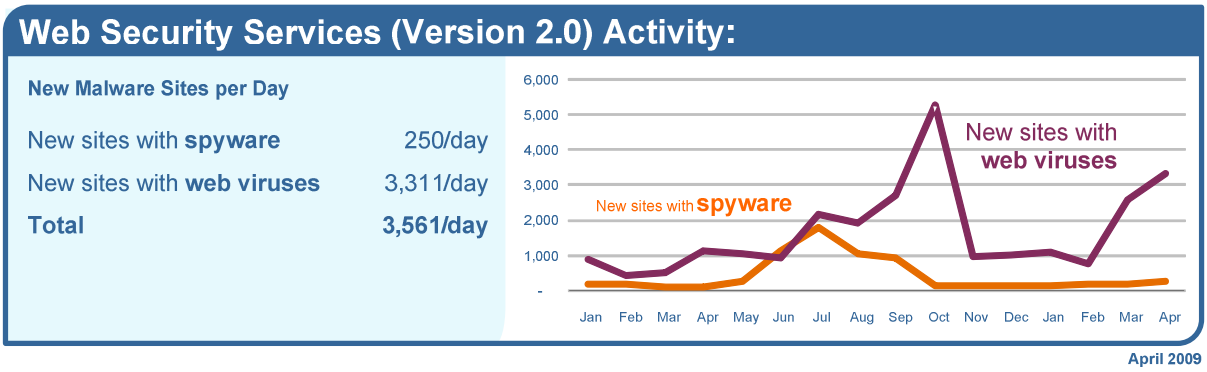
Web Security Services (Version 2.0) Activity:

Policy-Based Filtering		Web Viruses and Trojans		Potentially Unwanted Programs	
Advertisements & Popups	61.6%	Trojan.Win32.Agent.bxgd	29.8%	PUP:Cinmus	40.3%
Streaming Media	8.7%	Trojan-Downloader.JS.Iframe.aqo	21.9%	PUP:WebToolbar.Win32.MyWebSear...	26.9%
Games	4.6%	Generic.dx	9.5%	PUP:WebToolbar.Win32.Zango.bw	4.5%
Downloads	4.2%	Trojan-Downloader.JS.Agent.dwf	3.4%	PUP:AdWare.Win32.AdMedia.ed	4.0%
Chat	3.5%	Generic PWS.y	2.3%	PUP:SAHAgent	2.1%
Blogs & Forums	2.9%	Refpron.gen	2.0%	PUP:AdWare.Win32.BHO.gei	2.1%
Personals & Dating	1.8%	Trojan-Clicker.HTML.IFrame.zm	1.6%	PUP:ZangoSA	2.0%
Adult/Sexually Explicit	1.8%	Trojan.JS.Agent.xl	1.6%	PUP:AdWare.Win32.SearchPage	1.4%
Infrastructure	1.3%	JS/Tenia.d	1.6%	PUP:BDSearch	1.3%
Gambling	1.1%	JS/Obfuscated	1.3%	PUP:AdWare.Win32.Shopper.ar	1.0%

April 2009

In die Gefahrenklasse „Nicht klassifiziert“ fallen alle neuen und bisher noch nicht eingestuften Websites. Dazu können Seiten, die für betrügerische und anrüchige Zwecke wie beispielsweise Phishing und Spam verwendet werden, ebenso gehören wie gerade erst von Firmen mit tadellosem Leumund eingerichtete Web-Auftritte und Domains, die bis dato einfach noch nicht kategorisiert wurden. Durch Rückgriff auf den Service von MessageLabs 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.

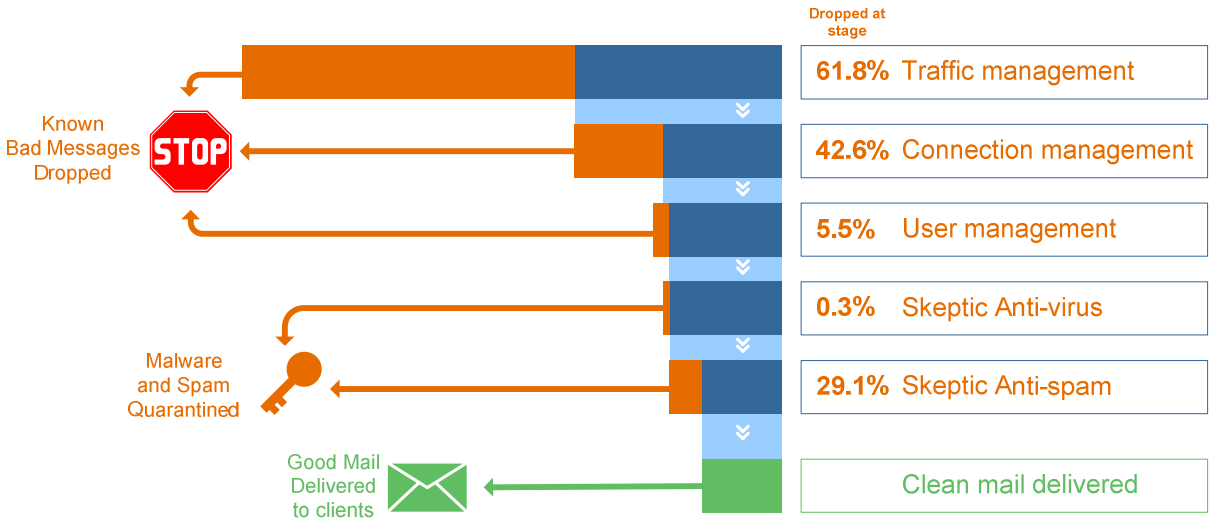
Das folgende Kurvendiagramm veranschaulicht, wie im Laufe des Monats April das Aufkommen an täglich neu zu sperrenden Spyware- und Adware-Seiten gestiegen ist und wie sich im Vergleich dazu die entsprechende Zahl der pro Tag blockierten Websites mit Viren und Trojanern entwickelt hat.



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 April wurden im Rahmen der MessageLabs-Dienste durchschnittlich 5,58 Milliarden SMTP-Verbindungen pro Tag verarbeitet. Davon wurden 61,8 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 April wurden auf diese Weise durchschnittlich 42,6 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 April wurden durchschnittlich 5,5 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.

Bei Rückfragen erreichen Sie uns unter: 0800 6647453

www.messagelabs.de

Ihr MessageLabs Team Skeptic™