

## „Storm“-Niedergang macht den Weg frei für neue Spam- und Malware-Trends; Reichweite der Botnets wächst

*Symantec veröffentlicht den MessageLabs Intelligence Security Report für das Jahr 2008*

München/Gloucester, 08. Dezember 2008 – Die Symantec Corporation (Nasdaq: SYMC) hat den neuen MessageLabs Intelligence Security Report für 2008 vorgelegt. Der aktuelle Jahresbericht zur Online-Sicherheit zeigt im Detail auf, dass 2008 in Bezug auf die Cyber-Security-Landschaft ein Schlüsseljahr war. Techniken zur Verbreitung von Malware und Spam durchliefen revolutionäre Fortschritte und prägten so die globale Schattenwirtschaft deutlich.

Die **Spam-Quote** erreichte ihren höchsten Wert im Berichtsjahr mit 82,7 Prozent bereits im Februar. Insgesamt belief sie sich 2008 auf 81,2 Prozent – verglichen mit 84,6 Prozent im Vorjahr. Immerhin 90 Prozent des gesamten Spam-Aufkommens wurden 2008 über Botnets verteilt. Dazu zählte auch das berüchtigte, Anfang 2007 aufgetauchte Storm-Botnet (auch unter dem Namen Peacomm bekannt). Dieses verschwand bis Ende des Jahres 2008 jedoch weitestgehend von der Bildfläche und machte rivalisierenden Botnets wie Srizbi oder Cutwail (beziehungsweise Pandex) Platz. Im September und November gelang dank der Zusammenarbeit mehrerer Behörden ein wichtiger Schlag gegen die Szene der Spammer und Cyber-Kriminellen: Ihren Geschäftsbetrieb einstellen mussten zwei US-amerikanische Internet Service Provider (ISPs), die bezichtigt wurden, das Hosting von Schaltzentralen einiger der größten Botnets betrieben zu haben. Dies galt unter anderem für Mega-D (oder Ozdok) und Srizbi, die zusammen für rund 50 Prozent des gesamten Spam-Aufkommens verantwortlich

**Pressekontakt:**

**Harvard Public Relations**

Stephanie Thaller

Patrick Yahya

t +49 (0)89 53 29 57-0

[Stephanie.Thaller@harvard.de](mailto:Stephanie.Thaller@harvard.de)

[Patrick.Yahya@harvard.de](mailto:Patrick.Yahya@harvard.de)

waren. Mit Ausnahme von Srizbi haben alle betroffenen Botnets mittlerweile Alternativen für das Hosting ihrer Command-and-Control-Server gefunden. Infolgedessen hat die Spam-Belastung wieder beinahe das frühere Niveau vor den Aktionen gegen die beiden ISPs erreicht, wobei insbesondere Botnets wie Cutwail und Rustock die Lücke von Srizbi füllen.

Im Laufe des Jahres 2008 haben Spammer zunehmend eine Vorliebe dafür entwickelt, ihre Kampagnen über die kostenlosen Online-Dienste großer und angesehener Anbieter zu verbreiten. Dabei legten sie es darauf an, die **CAPTCHA-Mechanismen** (Completely Automated Public Turing Tests to tell Computers and Humans Apart) von Webmail-Services und anderen via Internet nutzbaren Software-Anwendungen auszuhebeln und so eine riesige Zahl von Benutzerkonten für diese Angebote anzulegen. Stammte im Januar 2008 noch 6,5 Prozent des Spam-Aufkommens von solchen Accounts, so stieg dieser Anteil für den Rest des Jahres auf durchschnittlich etwa 12 Prozent. Seinen Höchststand erreichte er im September mit 25 Prozent.

„2008 war ein ganz entscheidendes Jahr für die IT-Sicherheits-Industrie: Neue Bedrohungen sind aufgetaucht und bekannte Angriffsformen wurden weiterentwickelt, während sich das Internet nun immer ausgereifter und differenzierter präsentiert und seine Anwender sich besser mit dem Web auskennen denn je“, betont Mark Sunner als Chief Security Analyst von MessageLabs und ergänzt: „Geknackte CAPTCHA-Tests haben sich als eine der wirksamsten Möglichkeiten für Spammer erwiesen, ihre Inhalte flächendeckend zu verteilen. Mittlerweile ging schon eine Vielzahl unterschiedlicher Spam-Kampagnen von kostenlosen Webmail-Diensten und Social-Networking-Portalen aus, die sich nur mit persönlichen Benutzerkonten nutzen lassen.“

Weite Verbreitung haben 2008 auch **komplexe Web-basierte Schadprogramme** gefunden, die sich unbemerkt auf den Rechnern ahnungsloser Anwender installieren, ohne dass diese dafür einen Download anklicken oder eine Datei öffnen müssten. Diese Art von Malware macht sich insbesondere die Web-Präsenzen von Online-Communities und die Sicherheitslücken eigentlich vertrauenswürdiger Internetseiten zunutze. So ist die Zahl der pro Tag im Durchschnitt neu entdeckten Websites, auf denen Schadprogramme hinterlegt waren, im Laufe des Jahres permanent gestiegen

– von 1.068 im Januar auf den Höchststand von 5.424 im November. Mussten 2007 täglich noch 1.253 neue Websites gesperrt werden, so waren es 2008 bereits 2.290. Dies ist vor allem eine Folge der vermehrten Attacken mittels SQL-Injection-Techniken.

Während also Web-basierte Angriffe im Laufe des Jahres 2008 an Popularität unter Online-Kriminellen gewonnen haben, ging die **Belastung des E-Mail-Verkehrs** mit Schadprogrammen gegenüber 2007 um 0,15 Prozentpunkte zurück. Im Berichtsjahr enthielten 0,70 Prozent aller E-Mails schadhaften Code. Das entspricht einem Anteil von 1 zu 143,8. Im Jahr zuvor hatte dieser noch 0,85 Prozent oder 1 zu 117,7 betragen. Weiterhin ist für das Jahr 2008 das Auftauchen von zwei unterschiedlichen Formen **gezielter Angriffe auf ausgewählte Opfer** zu konstatieren. Für das Berichtsjahr vermeldet MessageLabs, dass pro Tag 53 gezielt adressierte Trojaner abgefangen wurden. Besonders hoch war die Belastung mit solchen Attacken im April 2008, als täglich 78 von ihnen abzuwehren waren. Demnach setzt sich der Trend fort, dass die Zahl derartiger Fälle stetig zunimmt: Im Jahr 2005 waren es ein oder zwei pro Woche gewesen, 2006 dann ein oder zwei pro Tag und zu Beginn des Jahres 2007 schon zehn pro Tag.

„Mit Web 2.0 eröffnen sich Internet-Betrüggern quasi unendliche Möglichkeiten, um Viren und Trojaner zu verteilen – von gefälschten Benutzerkonten für Social-Networking-Seiten bis hin zu getürkten Videos. Und 2008 sind Angriffe über Social-Networking-Umgebungen bereits äußerst real geworden“, berichtet Mark Sunner und führt aus: „Das Web 2.0 floriert dank der Bereitschaft zahlloser Anwender, eigene Inhalte öffentlich bereitzustellen (Stichwort „**user generated content**“) – und davon profitiert zusehends auch die Spam-Szene. Eine der stärksten Waffen von Online-Kriminellen besteht heute darin, neue Medien und Kommunikationskanäle für ihre Zwecke zu adaptieren. Längst laden sie selbst scheinbar attraktive Inhalte hoch, die informationshungrige Anwender dazu verlocken, sie massenhaft anzuklicken. So gelingt es den Betrügern, Blendwerk und systematische Irreführung in ein funktionierendes Geschäftsmodell innerhalb der Schattenwirtschaft zu überführen.“

Ein gezielter, Ende Juli an die Sportverbände und -funktionäre mehrerer Teilnehmerländer der **Olympischen Spiele** verschickter Trojaner veranschaulicht, wie Angriffe dieser Art im Laufe des Jahres an Beliebtheit gewonnen haben.

Absender war angeblich eine an der Ausrichtung der Spiele beteiligte Organisation. Versteckt hatten die Urheber des Angriffs ihre Malware in einer angehängten Datei, in die JavaScript-Code eingebettet war, der als Virendropper ein ausführbares Programm auf dem Computer des Empfängers ablegte. Die Absender eines weiteren gezielten, in diesem Falle zum Zwecke der **Unternehmensspionage** verbreiteten Trojaners tarnten sich derweil als eine bekannte Wirtschaftsaufsichtsbehörde und gaben vor, einer Beschwerde gegen den jeweiligen Adressaten nachgehen zu müssen. Verschickt wurde betreffende Schadprogramm-Mail an rund 900 Führungskräfte von Unternehmen in aller Welt.

Gegen Ende des Jahres 2008 stieg zudem die Zahl der Angriffe, die sich der fortschreitenden **Kredit- und Finanzkrise** als Aufhänger und Türöffner bedienten. Spammer und Online-Betrüger versuchten demnach, ihren Profit aus der zunehmenden Panik und Ungewissheit vieler Verbraucher zu ziehen, die in Folge der Umwälzungen an der Wall Street und anderen Finanzplätzen rund um den Erdball zu beobachten war.

## **Lockende Bots und Social Networking**

2008 zeichneten Botnets nicht nur für 90 Prozent der gesamten Spam-Belastung verantwortlich, sondern sorgten auch dafür, dass ein größerer Prozentsatz der per E-Mail verbreiteten Malware-Angriffe auf Links zu entsprechenden Websites entfiel. Seinen höchsten Stand erreichte dieser Anteil mit 61,1 Prozent im Februar des Berichtsjahres, als das Storm-Botnet seine Schadprogramm-Aktivitäten intensivierte und hinter 96 Prozent der abgefangenen Links dieser Art stand. Vor seinem Niedergang lief eine der letzten Aktionen von Storm im Juli 2008 zum Teil darauf hinaus, einen neuen Schub an Malware zu verbreiten – dies erfolgte über E-Mails, die sich in ihren Betreffzeilen unter anderem auf zu Tode kommende **Prominente** bezogen und Links zu Schadprogramm-Seiten enthielten. Wer diese Websites aufrief, installierte auf seinem Rechner unbemerkt und ohne sein weiteres Zutun das als Anti-Spyware-Programm getarnte **Lockprogramm „Antivirus XP 2008“**. Die heruntergeladene Software startete dann jeweils einen vermeintlichen Suchlauf auf dem betreffenden Computer und bot an, die angeblich gefundenen Viren gegen Zahlung einer entsprechenden Gebühr zu entfernen. Nach dem Bedeutungsverlust von Storm wurden später auch über andere Botnets wie Srizbi, Rustock und Mega-D massenweise E-Mails mit Links zu dieser Lock-Software verschickt. Im Juli entfiel ein

---

Drittel aller Malware-Mails, die MessageLabs abgefangen hat, auf „Antivirus XP 2008“. Im August enthielten dann sogar 64 Prozent aller Schadprogramm-Mails einen Link zu einem Trojaner-Dropper, der dazu diente, die falsche Anti-Spyware-Software auf dem Rechner der Adressaten zu installieren. Zumeist handelte es sich bei den verschickten Lock-Mails um getürkte Grußkarten.

Eine weitere Technik, die sich 2008 großer Beliebtheit unter Cyber-Kriminellen erfreute, setzte auf die Verbreitung von Schadprogrammen über **Social-Networking-Portale**. Erstmals aufgetreten waren solche Aktivitäten – damals allerdings noch in lediglich geringer Zahl – bereits Ende 2007. Eine Herangehensweise, die in diesem Jahr stark an Popularität gewonnen hat, bestand darin, auf den Seiten von Online-Kontaktnetzwerken gefälschte Benutzerprofile anzulegen und über diese dann Links zu Schadprogrammen zu posten oder die persönlichen Authentisierungsdaten anderer User auszukundschaften. Denn sobald Spammer erst einmal die Login-Informationen eines fremden Benutzers in die Hände bekommen haben, können sie Kommentare auf den Seiten von Usern aus der jeweiligen Buddylist hinterlassen und über den geknackten Account zudem andere Adressaten mit Nachrichten eindecken. Genutzt wurde dies in den meisten Fällen zum Versand von Werbemails, die teilweise auch Links zu typischen Spam-Websites wie etwa Online-Shops für Medikamente enthielten. Darüber hinaus haben Kriminelle, die sich auf Social-Networking-Seiten unerlaubt Zugang zu legitimen Benutzerkonten verschaffen konnten, häufig rücksichtslos alle verfügbaren persönlichen Informationen geplündert, für gezielte Betrugsversuche gegen besagte User verwendet und dabei schweren Schaden angerichtet.

Und schließlich haben sich auch im Hinblick auf die Bedrohung durch **Phishing-Angriffe** im Jahr 2008 bemerkenswerte Veränderungen ergeben. Insbesondere ist festzustellen, dass der Einsatz spezialisierter Botnets zum Auskundschaften persönlicher Authentisierungsdaten nun gang und gäbe geworden ist. Und während die Intensität von Phishing-Attacken im Laufe des Berichtsjahres weitgehend stabil geblieben ist, haben die Hintermänner ihre Aktivitäten zusehends auf weitere potenzielle Opfer ausgedehnt: Mittlerweile zielen die Angriffe nicht mehr wie in der Vergangenheit nur auf Finanzinstitute und deren Kunden ab, sondern auch auf Jobvermittlungen und Online-Shops. Es steht zu erwarten, dass 2009 die Zahl spezialisierter Trojaner zum Missbrauch von Online-Banking weiter zunimmt.

## **Die wichtigsten Trends des Jahres 2008 im Überblick:**

**Web-Sicherheit:** 2008 hat MessageLabs täglich im Durchschnitt 2.290 neue Websites aufgespürt, auf denen Schadprogramme hinterlegt waren. Das sind 82,8 Prozent mehr als im Jahr zuvor, als pro Tag der Zugriff auf durchschnittlich 1.253 neue Malware-Seiten zu unterbinden war. Der Anstieg ist vor allem auf SQL Injection-Angriffe zurückzuführen.

**Spam:** Die Spam-Quote ging von 84,6 Prozent im Jahr 2007 um 3,4 Prozentpunkte auf nunmehr 81,2 Prozent im Berichtsjahr zurück. 2008 bestand der Großteil der unerwünscht verbreiteten Werbe-Mails aus reinen Text- oder HTML-Inhalten. Gleichzeitig stieg der Anteil des Spam-Aufkommens, das mit Hilfe von Benutzerkonten bei eigentlichen vertrauenswürdigen Anbietern von Webmail-Diensten und anderen Online-Anwendungen auf den Weg gebracht wurde.

**Viren:** 2008 belief sich der Anteil von virenverseuchten Nachrichten am gesamten E-Mail-Verkehr im Durchschnitt auf 0,70 Prozent oder 1 zu 143,8. Das sind 0,15 Prozentpunkte weniger als 2007, als die Viren-Quote noch 1 zu 117,7 beziehungsweise 0,85 Prozent betragen hatte. Dieser Rückgang ist darauf zurückzuführen, dass Internet-Kriminelle zunehmend statt der E-Mail andere Wege zur Verbreitung von Schadprogrammen bevorzugen. Dazu gehören das Hosting gefährlicher Inhalte auf speziellen Websites und die unbemerkte Malware-Installation nach dem „Drive by“-Prinzip.

**Phishing:** 2008 verbarg sich hinter 1 von 244,9 E-Mails (beziehungsweise 0,41 Prozent des gesamten E-Mail-Aufkommens) der Versuch, persönliche Authentisierungsdaten auszuspionieren. Im Jahr zuvor hatte die entsprechende Phishing-Quote noch 1 zu 156 betragen. Im Berichtsjahr erreichten die diesbezüglichen Aktivitäten ihren Höhepunkt im Februar, als pro 99,1 E-Mails ein Phishing-Angriff zu konstatieren war. Zurückzuführen war diese besonders hohe Gefährdung auf das gestiegene Angebot an per Plug-and-Play in Betrieb zu nehmenden Phishing-Bausätzen und die Tatsache, dass sich die Urheber solcher Attacken verstärkt der Dienste spezialisierter Botnets bedienen.

---

Der vollständige Jahresbericht von MessageLabs Intelligence liefert noch genauere Daten und Analysen zu den in dieser Pressemitteilung erläuterten Trends und Zahlen. Der Report steht unter der folgenden Adresse zum Download bereit: [http://www.messagelabs.com/Threat\\_Watch/Intelligence\\_Reports](http://www.messagelabs.com/Threat_Watch/Intelligence_Reports)

## **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).

## **Hinweis für Redakteure:**

Wenn Sie mehr über Symantec und seine Produkte erfahren möchten, dann besuchen Sie unser Online-Pressezentrum unter [www.symantec.com/presse](http://www.symantec.com/presse) Dort liegt auch Bildmaterial von Personen und Produkten für Sie bereit.

Symantec und das Symantec Logo sind Warenzeichen oder eingetragene Warenzeichen der Symantec Corporation in den USA und ihrer Tochtergesellschaften einigen anderen Ländern. Andere Firmen- und Produktnamen können Warenzeichen oder eingetragene Warenzeichen der jeweiligen Firmen sein und werden hiermit anerkannt.