Finden Sie uns auf facebook Folgen Sie uns auf twitter

AV-TEST The Independent IT-Security Institute Magdeburg Germany

AV-TEST-Studie:
Gefährliche Spam-Mails

Spam – gefährlicher denn je

Mit Hilfe von Botnetzen versenden Spammer täglich Millionen von Spam-Mails. Das Magdeburger Institut AV-TEST hat in einer 18-monatigen Studie über eine halbe Million Spam-Mails gesammelt und bewertet: die Gefahr, die von Spam ausgeht, ist so hoch wie noch nie.

Markus Selinger

Es ist ruhig geworden um Spam. Er ist weiterhin nervig, aber man hat sich an ihn gewöhnt. Genau dieser Umstand macht ihn nun umso gefährlicher. In einer 18-monatigen Studie, von August 2011 bis Februar 2013, hat das Labor von AV-TEST über eine halbe Million als Spam klassifizierte Mails gesammelt und analysiert. Das Ergebnis ist ernüchternd: jede dritte Spam-Mail, die einen Anhang hat, ist mit einem Schädling infiziert. Andere Mails versuchen den Anwender meist auf eine infizierte Webseite zu locken.

Viel schlimmer allerdings ist die Erkenntnis, dass 25 Prozent der Spam-Schleudern in Büros stehen – auch in deutschen!

Über 500.000 Spam-Mails in der Labor-Analyse

AV-Test hat insgesamt 550.000 Mails untersucht, die zuvor als Spam klassifiziert wurden. Davon waren knapp 14.000 Mails infiziert, das entspricht in etwa 2,5 Prozent.

Gesammelt wurde der Spam mit Hilfe 90 überwachter Mailaccounts. Zum Teil wurden die Mail-Adressen in Foren und Gewinnspielen eingetragen. Damit war der Grundstein gelegt – nach einer kurzen Anlaufzeit empfingen die Accounts täglich Dutzende von Spam-Mails.

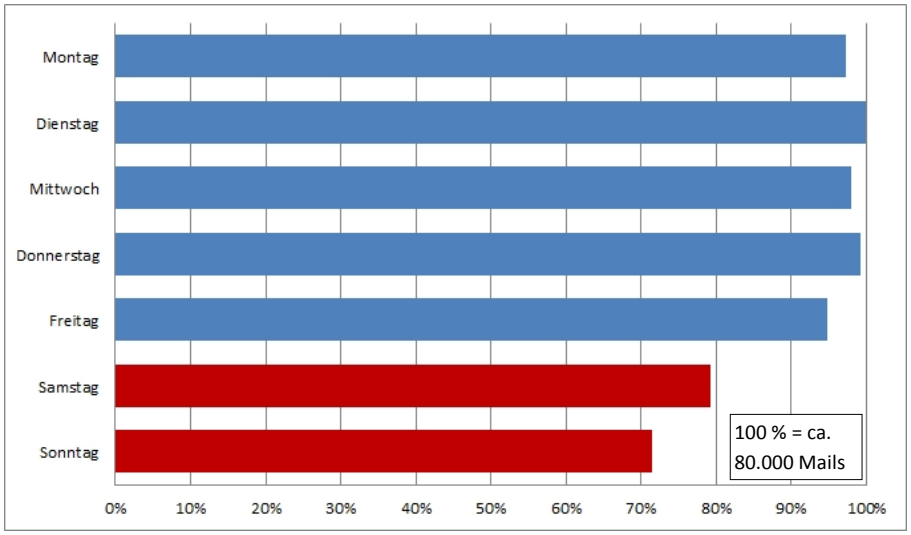
Viele infizierte Anhänge

Gut 30.000 der 550.000 analysierten Spam-Mails hatten einen Anhang, wovon über 10.000, also etwas über 30 Prozent, mit einem bösartigen Schädling bestückt waren. In 400.000 Mails fanden sich neben Text auch URLs, also Internetadressen. Bei den Mails mit URLs führte knapp 1 Prozent der Links direkt auf mit Schädlingen infizierte Seiten. Der Rest waren meist betrügerische Angebote für gefälschte Produkte, wie etwa Pharmazeutika.

Mehr Info unter www.av-test.de

Aktuelle Infos zum Test, weiteren Studien und aktuelle Statistiken zu Spam und Malware finden Sie immer online auf der Homepage der AV-TEST GmbH.

25 Prozent der Spam-Schleudern stehen in Büros!



Für die Studie wurde der Spam an jedem Wochentag registriert. Das Maximum lag bei etwa 80.000 Mails. Von Montag bis Freitag ist der Spam-Versand recht gleichmäßig. Am Wochenende fällt er deutlich ab. Das belegt: diese PCs stehen in Büros und sind am Wochenende ausgeschaltet. Somit stehen 25% der Spam verschickenden Botnetz-PCs in Büros – auch in deutschen!

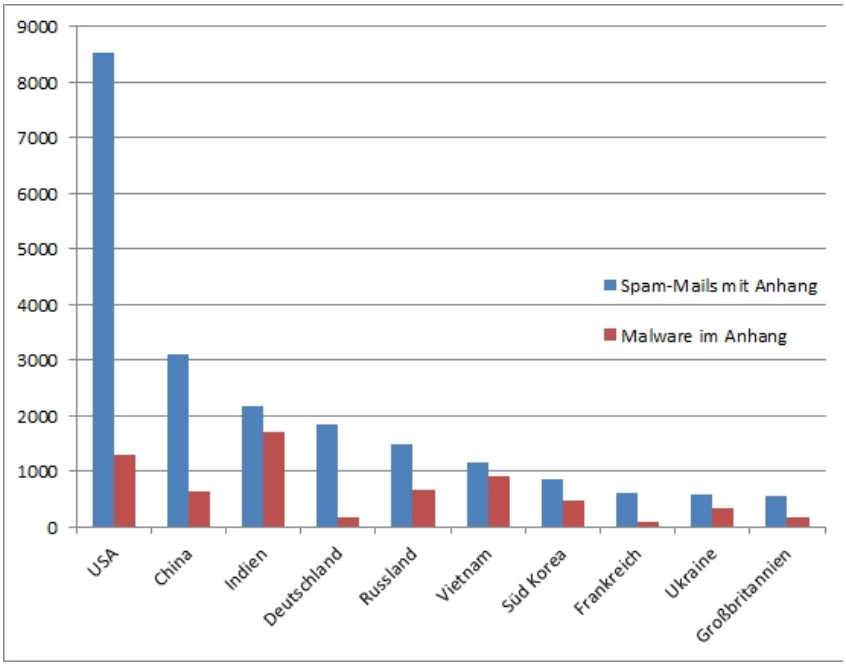
Bei den infizierten Mailanhängen fanden sich meistens die klassischen Vertreter: ZIP-Dateien, ausführbare EXE-, COM-, SCR-, BAT- oder PIF-Dateien und HTML-Dokumente für eine Attacke. Aber auch PDF-Dateien und Bilder sind weiterhin beliebt als infizierte Objekte. Die Studie belegt: sobald an einer Spam-Mail eine ZIP-Datei hängt, ist diese zu fast 100 Prozent verseucht. Bei den ausführbaren Dateien wie EXE oder PIF ist das ebenfalls der Fall. Die an die Spam-Mails angehängten HTML-Dokumente waren während der Studie zu über 80 Prozent verseucht.

Indischer Spam ist immer gefährlich

Die meisten Spam-Mails mit Anhängen stammten zwar aus den USA, diese waren aber nur nur zu 15 Prozent mit Schadsoftware verseucht. Kam die Mail hingegen aus Indien, dann waren die Anhänge während der Studie zu 78 Prozent infiziert. Knapp dahinter folgten Mails mit Anhängen aus Vietnam: 77 Prozent.

Von den 30.000 registrierten Spam-Mails mit Anhängen kam die Hälfte aus den USA, China, Indien und sogar Deutschland. Der deutsche Spam mit Anhang war aber nicht so gefährlich: 10 Prozent der Mails hatten einen Schädling mit im Gepäck.

Spam-Mails mit Anhang nach Ländern sortiert



Die USA waren zwar in der Studie der größte Versender von Spam-Mails mit Anhängen, aber sie hatten im Vergleich zu anderen Ländern weniger gefährliche Mitbringsel. Die Mails mit Absender aus Indien oder Vietnam hatten fast immer einen Schädling im Gepäck. Mails mit Anhängen aus Deutschland waren zu 10 Prozent verseucht.

25 Prozent der Spamschleudern stehen in Büros

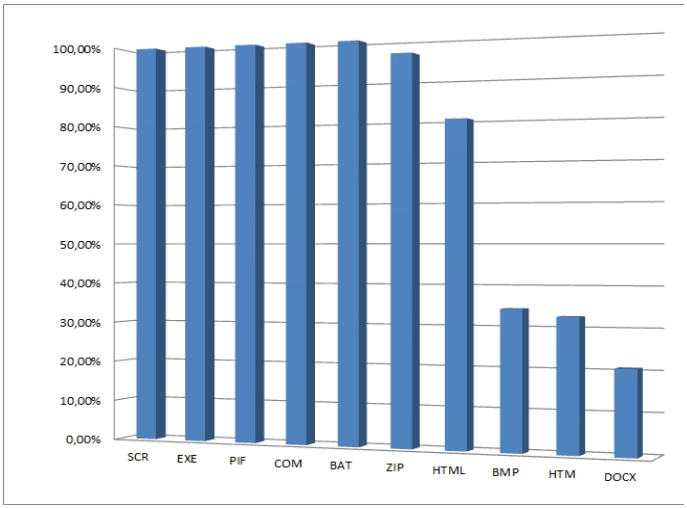
In der Studie wurde der Spam-Versand an jedem Wochentag registriert und zum Abschluss nach 18 Monaten analysiert. Das Ergebnis: von Montag bis Freitag hielt sich das Niveau an verschicktem Spam immer recht konstant. Am Wochenende, also Samstag und Sonntag, sank der Versand um 25 Prozent. Damit belegt die Studie, dass 25 Prozent der Spam-Schleudern in Büros stehen, wo sie am Wochenende abgeschaltet sind. Pünktlich am Montag steigt das Spam-Niveau wieder an.

Die Analyse nach Monaten zeigte keine Schwerpunkte. Es ließ sich nur feststellen, dass der Juli und der August die meisten Mails mit der höchsten Infizierungsrate hatten. Ein Muster war dabei aber nicht zu erkennen.

Botnetze – aktiv & hinterhältig

Der Versand der Spam-Mails erfolgt fast ausschließlich über PCs, die ganz unauffällig von Botnetzen ferngesteuert werden. Somit haben die Mails immer andere Versand-IPs. Dadurch haben Provider Schwierigkeiten, auffällige Mails anhand ihrer IP-Adresse schnell zu identifizieren.

Top Ten der verseuchten Mail-Anhänge



In der Studie wurden insgesamt 30 verschiedene Dateitypen als Mail-Anhang gezählt. Die Top Five zeigt, sobald an der Spam-Mail eine ausführbare Datei hängt, ist diese immer mit einem Schädling infiziert.

Die mit einem steuernden Trojaner infizierten PCs verhalten sich gegenüber dem Anwender perfide unauffällig. Schließlich soll dieser nicht merken, dass jemand seinen PC zum Mailversand nutzt. Botnetze haben auch eine sehr unterschiedliche Größe. Die bereits in den letzten Jahren lahmgelegten Netze hatten eine Größe von 1 bis 10 Millionen gesteuerter PCs. Davon waren zwar nie alle immer online, aber auch mit nur ein paar hunderttausend PCs lässt sich viel Spam in kürzester Zeit versenden.

„Bin ich Teil eines Botnetzes?“ Online-Check für den PC!

Das Bundesamt für Sicherheit bietet in Zusammenarbeit mit dem Verband der deutsche Internetwirtschaft die Webseite www.botfrei.de. Dort finden sich viele Hersteller-Links, mit denen sich überprüfen lässt, ob PCs zu einem Botnetz gehören.

Antivirensoftware schützt

Wird auf einem PC ein aktuelles Schutzpaket eingesetzt, so ist eine feindliche Übernahme des PCs durch ein Botnetz fast ausgeschlossen. Denn die Schutzpakete bringen auch einen Scanner für Rootkits und Trojaner mit – das sind die beliebtesten Werkzeuge von Botnetz-Betreibern. Die aktuellen Tests der besten Schutzpakete lassen sich auf www.av-test.de jederzeit kostenfrei nachlesen.

Finden Sie uns auf facebook Folgen Sie uns auf twitter

Magdeburg, den 09. April 2013
Autor: Markus Selinger

Bei weiteren Fragen wenden Sie sich bitte an das Team der AV-TEST GmbH.
Mail: presse@av-test.de
Tel.: +49 391 6075460
Web: www.av-test.de