

Rassisten-Wurm

Mit Hilfe des Wurms Sober.G wurden Millionen rassistischer Spams verschickt. Alle mit falschen Absendern, was unbescholtene Anwender ins Ziellicht brachte.

■ von Bruno Habegger

Piero regt sich fürchterlich auf. Jemand verschickt in seinem Namen übelste ausländerfeindliche E-Mails. «Dabei weiss jeder, dass ich ein Martin-Luther-King-Fan bin. Also genau das Gegenteil!», klagt er in der Newsgroup ch.admin. Auch im Namen des PCTipp ist derselbe Denkmüll verbreitet worden. Die Mails wurden um den 10. Juni, kurz vor der Europawahl, massenhaft in Umlauf gesetzt, auch in der Schweiz. Sie tauchen jetzt noch – wenn auch nicht mehr so häufig wie zu Beginn – in den Mailboxen auf.

Der Rassisten-Spam markiert einen Wendepunkt. Zum ersten Mal ist Spam – unverlangte Mails – nicht

nur lästig, sondern schädigt völlig unbescholtene Internetanwender. Die wahren Opfer sind diesmal nämlich nicht die Empfänger, sondern jene Menschen wie Piero, in deren Namen unversehens politische Propaganda verschickt wird. Sie verlieren an Ansehen und müssen sich unter Umständen rechtfertigen. Die Übeltäter sind noch unbekannt, dürften aber nach ersten Vermutungen aus der rechtsradikalen Ecke Deutschlands stammen.

Technisch ist die Sache klar: Schuld ist ein Trojaner namens Sober.H und dessen Wurm-Vorgänger Sober.G. Zuerst infizierte Sober.G Millionen von PCs. Der Wurm enthält eine Funktion, die selbstständig

Dateien aus dem Internet nachladen kann. Diese Funktion kann vom Entwickler des Wurms von aussen aktiviert werden. Sober.G lädt sich Sober.H herunter, der den Text der Nazi-Mails enthält. Daraufhin erhält Sober.G. den Befehl, sich zu deaktivieren. Jetzt tritt Sober.H in Aktion: Er verschickt die Propagandateile an alle E-Mail-Adressen, die er auf dem befallenen PC findet – ohne sich selbst an die Mailnachricht anzuhängen. So entwischen die Spams logischerweise auch allfällig vorhandenen Virenskannern beim Empfänger.

Perfiderweise setzt Sober.H beliebige gefundene E-Mail-Adressen auch ins Absender-Feld der Kopfzeile. So wird für die Empfänger der

Post aus Piero, dem Verehrer des Anführers der amerikanischen schwarzen Bürgerrechtsbewegung, ein tumbe Fremdenhasser.

Fazit: Es ist keineswegs so, dass der Absender der Nazi-Mail einen PC hat, auf dem der Wurm wütet. Lediglich seine Adresse ist auf irgendeinem von Sober.G verseuchten PC erfasst. Und: Die Mail ist gar nie vom angeblichen Absender verschickt worden.

Details zur Sober-Wurmfamilie lesen Sie im PCTipp-Virenticker, [WEBCODE 26136](#).

Anwender können sich schützen und mithelfen, das Sober-Netz stillzulegen. Als Erstes sollten Sie Ihre Sicherheitsmassnahmen überprüfen, den Virenskanner aktualisieren und den PC einem intensiven Virentest unterziehen. Achten Sie auch auf «Krankheitssymptome»: Wenn der Rechner ohne erkennbaren Grund plötzlich nur noch träge reagiert, könnte Sober aktiv sein. Verdächtig ist auch, wenn trotz geschlossenen Internetprogrammen die Lämpchen am Internetzugangsgesamt munter weiterblinken.

Laden Sie sich ein spezielles Tool herunter, das einzig dem Zweck dient, einen allfällig installierten Sober-Wurm zu entdecken und zu entfernen. Jenes von Symantec finden Sie zum Beispiel hier: <http://securityresponse.symantec.com/avcenter/FixSober.exe>. Eine Anlaufstelle ist auch die Security-Site von Microsoft: www.microsoft.com/security. Installieren Sie eine Firewall-Software wie zum Beispiel ZoneAlarm (www.zonealarm.de), beachten Sie dazu auch den Artikel «Alarmstufe Rot!», S. 28. Noch besser schützt eine Hardware-Firewall.

Mehr zum Thema Virenbekämpfung lesen Sie im PCTipp 4/2004, «Tipps gegen den Virenkater», S. 28, online unter www.pctipp.ch mit [WEBCODE pdf040428](#).

Fachleute konstatieren generell eine enorme Zunahme der Spam-Plage. Das Sicherheitsunternehmen Message Labs hat im Mai dieses Jahres im Auftrag seiner Kunden 909 Millionen E-Mails auf Virenbefall untersucht. Und stellte ganz nebenbei schockiert fest: Drei Viertel der Nachrichten waren Spam.

Herkömmliche Spam-Filter wie z. B. SpamPal helfen gerade bei den Nazi-Spams nicht weiter. Immerhin sind Sie als Anwender dank der Filterfunktion in Ihrem Mailprogramm der Spam-Flut nicht gänzlich hilflos ausgeliefert, da sich die-

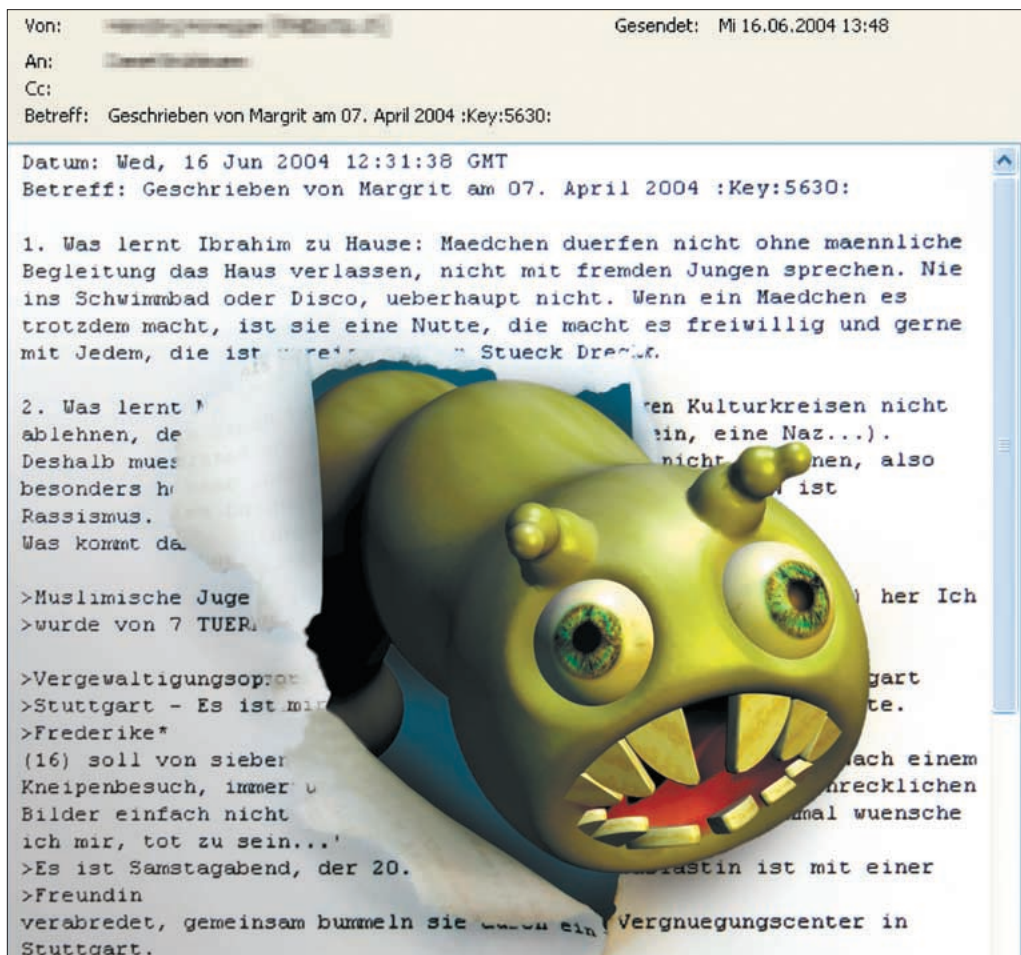


ILLUSTRATION TOM HUBSCHER, TNT-GRAPHICS

se Mails nur mit insgesamt rund 20 Betreff-Zeilen verschicken, siehe Box «Vorlagen für den Spam-Filter». Erstellen Sie eine Regel, die nach diesen Zeilen sucht, und lassen Sie die Mails automatisch löschen. In Outlook ist es der Regelasistent, mit dessen Hilfe Sie fein abgestuft darüber entscheiden, welche Mails in welchem Ordner landen und welche sofort gelöscht werden. Eine Kurzanleitung finden Sie auf www.pctipp.ch mit **WEBCODE 24140** und im PCTipp 4/2003, «Ganz einfach!», S. 62 (**WEBCODE pdf030462**).

Mit dem Regelasistenten haben Sie auch die Möglichkeit, Positiv-Listen zu erstellen. Das sorgt für die beste Ordnung im Postfach: Machen Sie mit Ihren Bekannten ein möglichst kryptisches Codewort in der Betreffzeile ab. Darauf setzen Sie den Filter an und leiten die Mails mit dem Codewort in der Betreffzeile in einen Ordner um. In diesem Ordner befinden sich künftig mit Sicherheit erwünschte Mails.

Gegen die eigentlichen Spam-Urheber lässt sich nichts unternehmen – wohl aber gegen jene PCs, die sich vom Besitzer *unbemerkt* als Spam-Schleuder betätigen. Informieren Sie die Provider, in dessen Netz die jeweiligen PCs aktiv sind. Dazu müssen Sie sich den Mail-Header (die Mail-Kopfzeile) der Spam-Nachricht anschauen. In Outlook blenden Sie den Header nach einem Rechtsklick auf die Nachricht im

BETREFF-ZEILEN

Vorlagen für den Spam-Filter

Wenn Sie nach den folgenden Betreff-Zeilen filtern, werden Sie künftig weniger stark von den Polit-Spams belästigt.

- Auslaenderanteile in Schweizer Gefaengnissen
- Bin ich zu weltfremd? Ich glaube wohl kaum
- Libanesen in Berlin
- Auslaendergewalt: Herr Rau, wo waren Sie?
- Moschee-Bau in Deutschland
- Neue Voelkerwanderung droht!
- Wer an ein Tabu ruehrt, muss und darf vernichtet werden
- Das kann unmoeglich sein -Leserbrief-
- Nein zum Zuwanderungsgesetz !
- EU Beitritt der Tuerkei ?
- Bankrott des Gesundheitswesens durch Auslaender!
- Paradies Bundesrepublik - Rente fuer die Welt -
- Richter unterstuetzt kriminelle Auslaenderin
- EU gibt Erwerbslosen volle Freizuegigkeit
- Polizei traute sich nicht, kriminellen Auslaender festzunehmen
- TUERKEN-TERROR AM HIMMELFAHRTSTAG
- Skandalurteil in Darmstadt
- SEHBEHINDERTER VON AUSLAENDERN VERPRUEGELT
- Was Deutschland braucht, sind deutsche Kinder!
- Auslaenderkriminalitaet steigt weiter!

Menüpunkt OPTIONEN ein. Halten Sie hier Ausschau nach Registern und Schaltflächen wie QUELTEXT oder KOPFZEILEN. Die IP-Adresse des PCs (Fachchinesisch siehe S. 36), der den Spam verschickte, steht im «Received»-Abschnitt. Manchmal ist nur eine Adresse zu finden, manchmal sind es mehrere. Wie man Mails sezziert, lesen Sie unter **WEBCODE pdf020740**. Alles übers Header-Lesen finden Sie unter www.th-h.de/faq/headerfaq.html.

Unter www.iks-jena.de/cgi-bin/whois erfahren Sie, wem die IP-Adresse gehört, und meist auch, wie die E-Mail-Adresse der Abuse-Abteilung des Providers lautet – dort werden Ihre Reklamationen dieser Art erledigt.

Schreiben Sie eine E-Mail, kopieren Sie den Text der Mailnachricht inklusive Header hinein und ergänzen Sie das Ganze mit der netten Bitte, das absendende System abzuklemmen. ■

MEINUNG

Taugt Linux schon als Windows-Ersatz?

Linux ist derzeit in und soll Windows schlagen. Das freie Betriebssystem taugt – mit leichten Einschränkungen – im Heimbereich bereits heute als Windows-Ersatz.

Microsoft und Windows benötigen dringend eine echte Konkurrenz. Die wächst mit Linux langsam, aber sicher heran. Ein schwer zu fassender Gegner für Bill Gates:

Linux ist keine Firma, die man aufkauft, sondern ein von vielen Freiwilligen weltweit entwickeltes Betriebssystem mit beliebig austauschbaren Elementen.

Das macht es flexibel. Dies und der Umstand, dass die meisten Programme und Elemente von Linux gratis erhältlich sind, erweisen sich als Stärke. Leider aber auch als Schwäche: Distributoren – Firmen, welche die Programme bündeln,



Bruno Habegger,
Redaktor

mit Konfigurations-Programmen und Supportleistungen ergänzen – benötigen viel Geld und ein hohes Qualitätsbewusstsein, um die sprudelnde Programmier-Kreativität der Linux-Szene in ein Windows-ähnliches PC-Erlebnis umzusetzen. Anwender merken schnell: Linux ist ein ungeschliffener

Diamant. **Ein Betriebssystem mit einigen rauen Ecken und Kanten und einer schier unerschöpflichen Auswahl an Programmen.** Manche beleidigen zwar Windows-verwöhnte Augen, weil der Entwickler flink programmiert, aber nichts von Design und Marketing versteht. Gelegentlich treten unschöne Fehler

auf, hier ein fehlendes Icon, da ein schlecht integriertes Programm. Doch meist handelt es sich um Kleinigkeiten, die mit steigender Erfahrung des Anwenders leicht ausgeglichen werden können. Und die Mühe wird durch ein Plus an Sicherheit gegenüber Windows, das einem steten Viren- und Wurmhagel ausgesetzt ist, mehr als aufgewogen.

Fazit: Wer sich vor dem Hardware-Kauf über die Linux-Kompatibilität informiert, einige Wochen Umgewöhnungszeit investiert und sich über kleinere Fehler nicht ärgert, der wird Windows nicht vermissen. Mehr zu Linux erfahren Sie im PCTipp-Kauf-Spezial das am 7. September erscheint.

KURZINFOS

CHIPSÄTZE

Intel hat die beiden neuen Desktop-Chipsätze 915 und 925 veröffentlicht (bisher Grantsdale und Alderwood genannt). Sie bringen Unterstützung für neue Technologien wie PCI-Express und DDR2-Speicher. Gleichzeitig sind sechs passende Pentium-4-Prozessoren erschienen.

GRATIS-OFFICE

OpenOffice.org wartet mit ähnlichen Anwendungen wie Microsoft Office auf, ist aber kostenlos. Die neue Version 1.1.2 ist auf der PCTipp-Website erhältlich (**WEBCODE 21031**). Sie bügelt diverse Bugs des Vorgängers aus.

VIREN-SCHUTZ

Microsoft will ein eigenes Antiviren-Produkt entwickeln. Es basiert wahrscheinlich auf einer Technologie der rumänischen Firma GeCAD, die der Software-Riese letztes Jahr geschluckt hat. Wann genau die neue Lösung auf den Markt kommt, ist noch unbekannt.

GOOGLE-KONKURRENZ

Unter www.seekport.de kann eine neue Suchmaschine für den deutschen Sprachraum getestet werden. Die Betreiber brüsten sich damit, den grössten deutschsprachigen Gesamtindex zu verwenden. Er wird von einem eigenen lokalen Team gepflegt.

PREISENKUNUNG

Die Swisscom reduziert per 1. Juli die Preise für die Mobilfunktechnologie GPRS. Diese kommt beim Surfen und Herunterladen von Daten zum Einsatz. Nach der Preissenkung kostet der Datentransfer pro 10 KB statt 19 nur noch 10 Rappen bzw. statt 30 noch 15 Rappen (Natel easy).

SCHUL-WINDOWS

Microsoft hat mit der Schweizerischen Fachstelle für Informationstechnologien im Bildungswesen einen Vertrag über fünf Jahre abgeschlossen. Das Software-Haus beteiligt sich am Aufbau eines technischen Supportzentrums. Ausserdem können Primarschulen Programme des Software-Konzerns künftig deutlich günstiger beziehen.