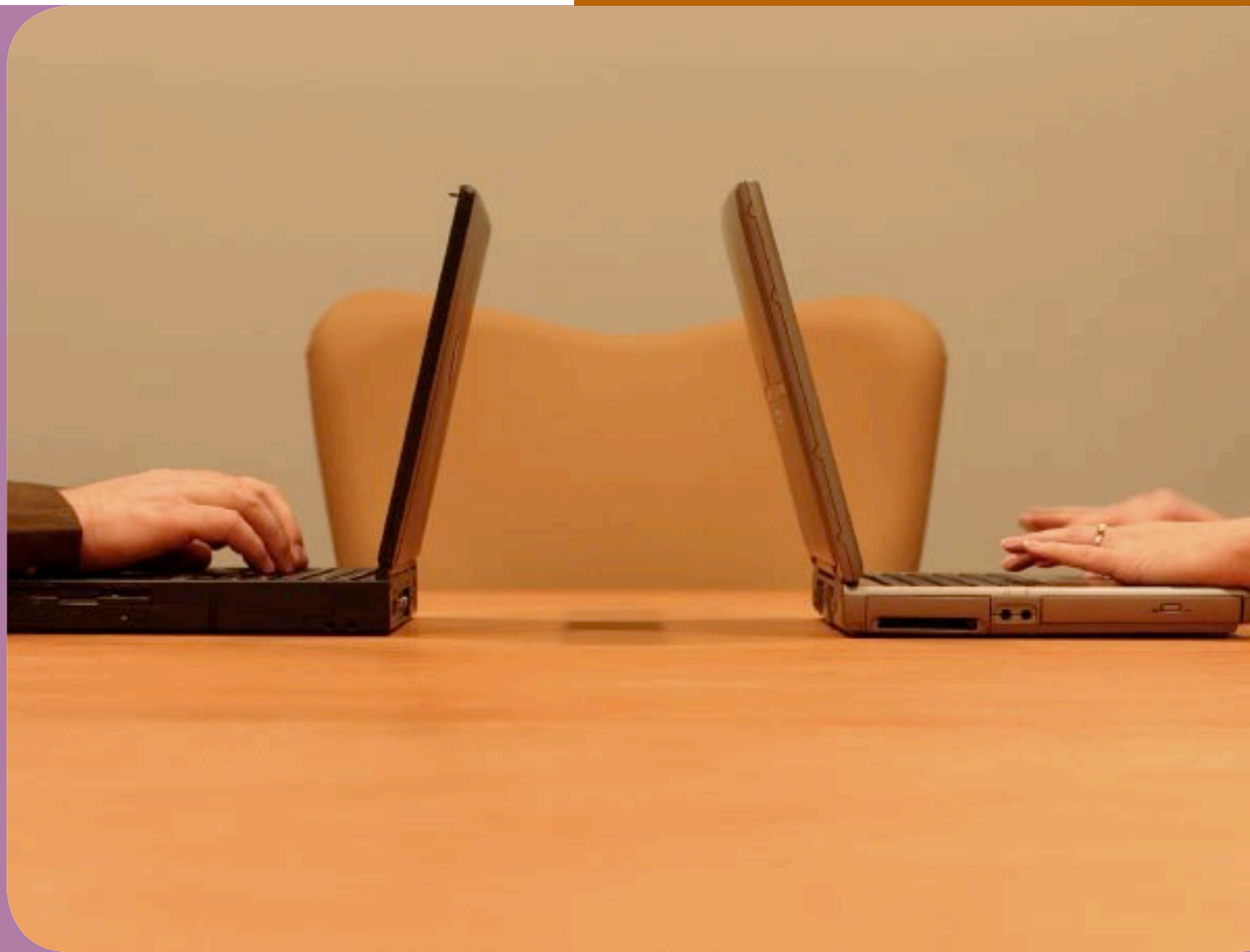
Risiko Tauschbörse: Was Ihre IP-Adresse verrät

CHIP Communications GmbH

Klicken, Lesen, Weitermachen. So einfach geht das.

Rubrik	**Internet**
Thema	**Sicherheit**
Umfang	**14 Seiten**
eBooklet	**00616**
Preis	**2,95 Euro**
Autor	**CHIP Communications GmbH**

Mit Hilfe von Fachbüchern kann man eine Menge lernen. Das ist gut. Wenn man genügend Zeit hat. Für die anderen Momente gibt es **eload24:** Digitale Bücher ohne jeden Ballast zu exakt definierten Themen, geschrieben von etablierten Fachautoren, unschlagbar preiswert und zum direkten Download. So bekommen Sie immer exakt die Informationen, die Sie wirklich brauchen. 24 Stunden am Tag.



Risiko Tauschbörse: Was Ihre IP-Adresse verrät

CHIP Communications GmbH

eload24 AG
Sonnenhof 3
CH-8808 Pfäffikon SZ

info@eload24.com
www.eload24.com

Inhalt

Risiko Tauschbörse: Was Ihre IP-Adresse verrät

Millionen von Menschen surfen täglich im Internet, und viele glauben, sie seien dabei anonym. Fataler Irrtum: Per IP-Adresse ist jeder User identifizierbar – auch Raubkopierer und Spammer.

Glaubt man der Musikindustrie, entsteht durch Raubkopierer allein in Deutschland jährlich ein Schaden im dreistelligen Millionenbereich. Kein Wunder, dass Musiktauschbörsen verstärkt ins Visier der Ermittlungen geraten.

Wichtigstes Beweisstück der Strafverfolgung ist die IP-Adresse. Denn wie eine Telefonnummer lässt sich die Adresse einem Anschluss und damit auch einem Nutzer zuordnen. Doch nicht nur Strafverfolger interessieren sich für die IP, auch Hacker und neugierige Webmaster. CHIP zeigt Ihnen in diesem eBooklet, wie eine IP-Adresse aufgebaut ist, was die IP über Sie verrät und wie Tauschbörsennutzer und Spammer enttarnt werden.

IP-Adressen: Aussehen und Verteilung im Internet

IP-Adressen gehören zum Alltag im Internet. Doch für viele ist die IP nicht mehr als ein abstrakter Begriff.

Dabei ist sie allgegenwärtig. Denn hinter jeder Verbindung steckt auch eine IP-Adresse – etwa wenn Sie eine Webseite aufrufen. In dem kurzen Moment zwischen dem Drücken der Return-Taste und dem Aufruf der Webseite beginnt die Kommunikation auf IP-Basis: Der Rechner schickt den Seitennamen an einen DNS-Server, und der antwortet mit einer IP-Adresse. Diese Adresse verrät dem Browser, auf welchem Webserver die Seite zu finden ist.

Doch damit nicht genug: Damit der Inhalt der Webseite überhaupt im Browser erscheinen kann, werden die Daten ebenfalls an eine IP-Adresse geschickt – die des Rechners. Jedes Gerät im Internet besitzt also eine IP-Adresse, die sich aber auch ändern kann.

Provider unterscheiden üblicherweise zwischen zwei Typen: Da wären zum einen die festen IP-Adressen. „Fest" bedeutet, dass die Adresse über einen längeren Zeitraum gleich bleibt. Solche Adressen werden in der Regel an Server und Router vergeben. Ein typisches Beispiel für einen Router mit fester IP-Adresse ist ein Firmennetzwerk. Jeder Mitarbeiter, der ins Internet geht, tut dies über den Router, der mit dem Provider verbunden ist.

Die Folge: Jeder Mitarbeiter hinterlässt auf jeder Webseite dieselbe IP-Adresse.

Ganz anders verhält es sich beim zweiten Adresstyp, der dynamischen IP-Adresse. Da

die Zahl der verfügbaren IP-Adressen begrenzt ist, bekommt jeder Provider einen Pool mit Adressen, mit dem er auskommen muss. In vielen Fällen reicht dieser Pool nicht aus, um jedem Kunden eine eigene IP-Adresse zu geben. Zwar besteht eine IP aus viermal drei Ziffern – das sind rein rechnerisch 4,3 Milliarden Adressen –, doch zahlreiche Regeln und Ausnahmen schränken den nutzbaren Zahlenraum ein. So verbleiben am Ende nur einige Millionen Adressen, die sich sämtliche Internetprovider weltweit teilen müssen.

Die Folge: Die IP ist einem Anschluss nur zugeordnet, solange der die Verbindung mit dem Provider aufrechterhält. Anschließend wird sie wieder freigegeben, und der nächste Kunde bekommt diese IP-Adresse. Trotzdem lässt sich eine IP-Adresse eindeutig einem bestimmten Anschluss zuordnen. Denn in Deutschland ist aufgrund des Vorratsdatenspeicherungsgesetzes jeder Provider verpflichtet, Protokoll zu führen. Gespeichert werden die Uhrzeit und die Kundennummer des Nutzers – sechs Monate lang. Für die Musikindustrie ist das ein wahres Geschenk: So lassen sich Tauschbörsennutzer auch noch Wochen später identifizieren.

Profitipp: Ein- und ausgehende IP-Adressen checken

Sowohl unter Linux als auch unter Windows lässt sich mit relativ einfachen Mitteln herausfinden, mit welchen IP-Adressen Ihr PC gerade kommuniziert.

Netstat

Das am schnellsten verfügbare Tool ist die On-Board-Software netstat. Öffnen Sie die Kommandozeile, und geben Sie den Be-

fehl „netstat -na" ein. Mit dem Parameter *-n* verhindern Sie, dass das Tool versucht, aus jeder IP-Adresse einen DNS-Namen zu machen – und der Aufruf deshalb quälend langsam wird. Der Parameter *-a* sagt dem Tool, dass Sie sämtliche Verbindungen sehen möchten. Andernfalls zeigt das Tool lediglich die Verbindungen Ihres Benutzerkontos an und nicht auch die vom System gestarteten.

TCPView

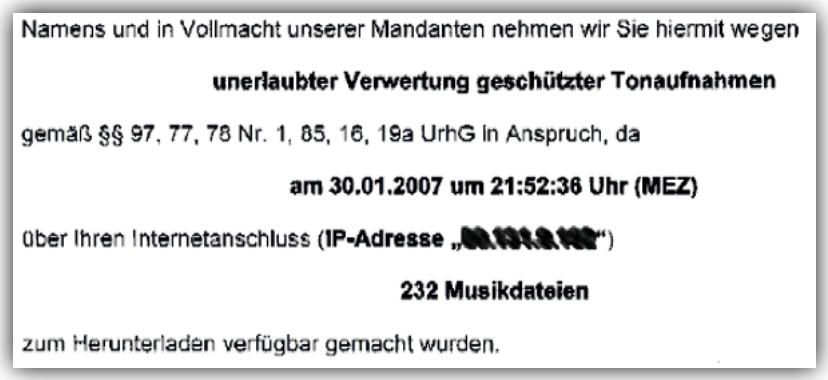
Wesentlich komfortabler als netstat ist dieses Tool von Sysinternals. Dank einer grafischen Oberfläche sowie einiger guter Features finden Sie mit TCPView im Handumdrehen nicht nur heraus, mit welchen IP-Adressen Ihr Rechner gerade in Verbindung steht, sondern auch, welche Anwendung diese Verbindung geöffnet hat. So lassen sich sogar Trojaner enttarnen, die im Augenblick mit dem Hacker kommunizieren.

P2P: Was BearShare und BitTorrent über Sie verraten

Noch gilt der Download von Raubkopien von einer Webseite als rechtliche Grauzone. Denn wer nicht selber Raubkopien verteilt, kann für den Vertrieb nicht belangt werden. In solchen Fällen konzentrieren sich die Rechteinhaber deshalb auf den Betreiber der Download-Webseite.

Ganz anders verhält es sich beim Filesharing. Denn an dieser Stelle ist jeder Teilnehmer der sogenannten Peer-to-Peer-Netzwerke (P2P) Empfänger und Sender zugleich. Für die Musik- und Filmindustrie ist das ein echtes Problem. Denn wenn ein illegales Angebot aus dem Netz verschwinden soll, reicht es nicht mehr, nur einen Server abzuschalten. Vielmehr muss jeder Teilnehmer, der eine Raubkopie besitzt, seinen Rechner vom Netz

nehmen, damit das Angebot verschwindet. Aus diesem Grund beauftragt die Industrie Firmen, die sich darauf spezialisiert haben, Filesharing-Nutzer ausfindig zu machen. Und im Prinzip ist das eine sehr leichte Aufgabe.



Namens und in Vollmacht unserer Mandanten nehmen wir Sie hiermit wegen

unerlaubter Verwertung geschützter Tonaufnahmen

gemäß §§ 97, 77, 78 Nr. 1, 85, 16, 19a UrhG in Anspruch, da

am 30.01.2007 um 21:52:36 Uhr (MEZ)

über Ihren Internetanschluss (**IP-Adresse „[redacted]“**)

232 Musikdateien

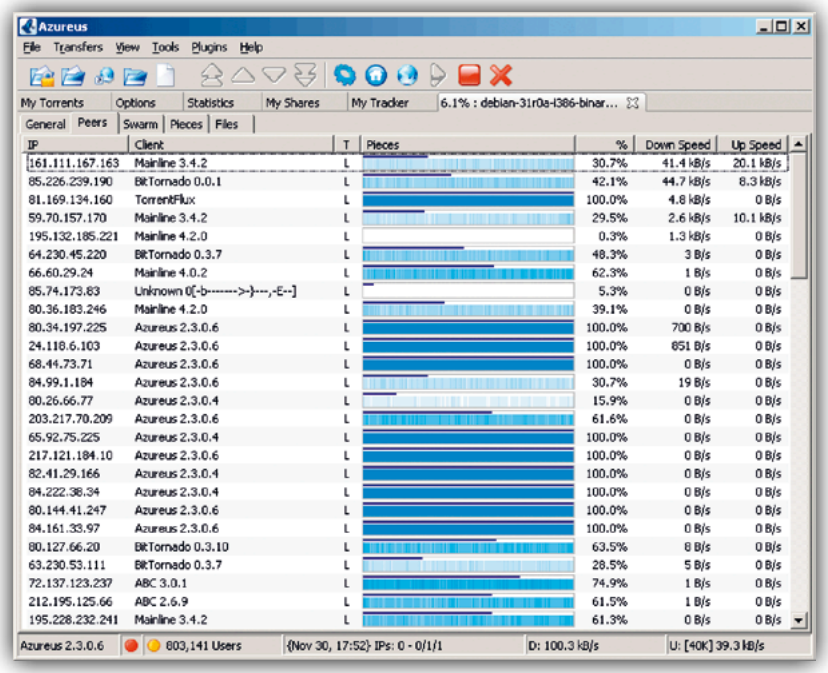
zum Herunterladen verfügbar gemacht wurden.

Erwischt: Zuerst lässt die Musikindustrie den Täter ausfindig machen, danach bekommt der Tauschbörsenteilnehmer eine Anzeige zugestellt – wie in diesem Fall.

Denn um an die IP-Adressen der Nutzer zu kommen, müssen sich die Ermittler nur in die zumeist offenen Netzwerke einklinken und die Adressen auslesen. Besonders einfach ist das bei Programmen wie Emule, BearShare und Limewire, die das Gnutella-Protokoll verwenden. Denn im Gegensatz zu anderen P2P-Protokollen wie BitTorrent lassen sich bei Gnutella Suchanfragen in das Filesharing-Netz schicken. Der Ermittler braucht nur den Namen eines urheberrechtlich geschützten Songs einzugeben und erhält eine Liste aller IP-Adressen, die diesen Song illegalerweise anbieten. Zudem kann er eine IP-Adresse eingeben und erfährt, welche Dateien dort zum Download angeboten werden.

Mit den gesammelten Informationen und der genauen Uhrzeit ist es dann kein Problem mehr, den Nutzer der Tauschbörse ausfindig zu machen. Gibt man die IP-Adresse etwa auf einer Seite wie www.dnsstuff.com ein und führt einen sogenannten WHOIS-Lookup durch, erfährt man im Handumdrehen, zu welchem Providerpool die IP-Adresse ge-

hört – inklusive Ansprechpartner, Telefonnummer und E-Mail-Adresse. Der Provider wiederum kann aufgrund der Vorratsdatenspeicherung die IP-Adresse anhand der Uhrzeit problemlos einem Kunden zuordnen.



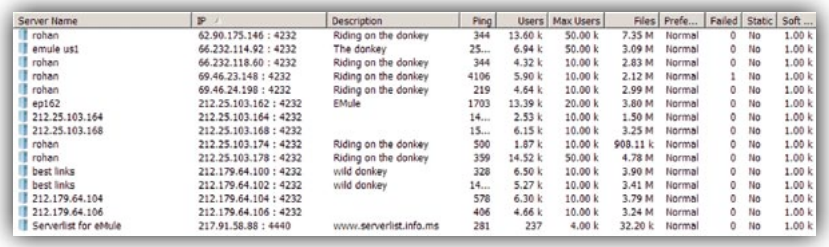
BitTorrent: Der Azureus-Client gibt bereitwillig Auskunft darüber, welche IP-Adressen die Tauschpartner haben.

Das funktioniert zwar nicht nur bei Gnutella, doch BitTorrent etwa erschwert die Ermittlungen ungemein. Grund: BitTorrent ist zwar auch ein offenes Filesharing-Protokoll, es lässt sich aber nicht durchsuchen.

Ein Beispiel: Um ein Musikalbum per BitTorrent herunterzuladen, ist zunächst eine Torrent-Datei erforderlich. Die finden die Tauschbörsennutzer in der Regel auf einer offenen Webseite wie ThePirateBay. Wird die Torrent-Datei nur einem kleinen, exklusiven Kreis zugänglich gemacht, so endet an dieser Stelle das Glück der Ermittler. Doch selbst wenn die Torrent-Datei zugänglich ist, hilft das nicht viel. Denn sie enthält nur die Dateinamen aus dem Musikalbum und die IP-Adresse eines sogenannten Trackers. Der Tracker ist zwar zentraler Bestandteil von BitTorrent, er bietet aber selbst keine Downloads an. Vielmehr führt der Tracker nur eine große Liste

aller IP-Adressen der aktiven Teilnehmer. Die Teilnehmer selbst teilt der Tracker in kleine Gruppen auf. Das soll verhindern, dass alle Teilnehmer miteinander kommunizieren müssen und dadurch ein unnötiger Verwaltungsaufwand entsteht. Wer sich also an einem Torrent beteiligt, bekommt eigentlich niemals sämtliche IPs zu Gesicht – es sei denn, es handelt sich nur um wenige Teilnehmer.

Oberstes Ziel der Musikindustrie ist es deshalb, die Tracker und Torrent-Webserver aus dem Internet zu nehmen. Das gestaltet sich aber zumeist recht schwierig, da manche Länder die Tracker nicht gesetzlich verbieten können. Da auch BitTorrent nicht anonym ist, müssen die Teilnehmer jedoch damit rechnen, entdeckt und verfolgt zu werden.



Server Name	IP	Description	Ping	Users	Max Users	Files	Prefe...	Failed	Static	Soft ...
rohan	62.90.175.146 : 4232	Riding on the donkey	344	13.60 k	50.00 k	7.35 M	Normal	0	No	1.00 k
emule us1	66.232.114.92 : 4232	The donkey	25...	6.94 k	50.00 k	3.09 M	Normal	0	No	1.00 k
rohan	66.232.118.60 : 4232	Riding on the donkey	344	4.32 k	10.00 k	2.83 M	Normal	0	No	1.00 k
rohan	69.46.23.148 : 4232	Riding on the donkey	4106	5.90 k	10.00 k	2.12 M	Normal	1	No	1.00 k
rohan	69.46.24.198 : 4232	Riding on the donkey	219	4.64 k	10.00 k	2.99 M	Normal	0	No	1.00 k
ep162	212.25.103.162 : 4232	EMule	1703	13.39 k	20.00 k	3.80 M	Normal	0	No	1.00 k
212.25.103.164	212.25.103.164 : 4232		14...	2.53 k	10.00 k	1.50 M	Normal	0	No	1.00 k
212.25.103.168	212.25.103.168 : 4232		15...	6.15 k	10.00 k	3.25 M	Normal	0	No	1.00 k
rohan	212.25.103.174 : 4232	Riding on the donkey	500	1.87 k	10.00 k	908.11 k	Normal	0	No	1.00 k
rohan	212.25.103.178 : 4232	Riding on the donkey	359	14.52 k	50.00 k	4.78 M	Normal	0	No	1.00 k
best links	212.179.64.100 : 4232	wild donkey	328	6.50 k	10.00 k	3.90 M	Normal	0	No	1.00 k
best links	212.179.64.102 : 4232	wild donkey	14...	5.27 k	10.00 k	3.41 M	Normal	0	No	1.00 k
212.179.64.104	212.179.64.104 : 4232		578	6.30 k	10.00 k	3.79 M	Normal	0	No	1.00 k
212.179.64.106	212.179.64.106 : 4232		406	4.66 k	10.00 k	3.24 M	Normal	0	No	1.00 k
Serverlist for eMule	217.91.58.88 : 4440	www.serverlist.info.ms	281	237	4.00 k	32.20 k	Normal	0	No	1.00 k

Tauschserver: Auch die Teilnehmer des Emule-Netzwerks müssen fürchten, über ihre IP-Adresse identifiziert zu werden.

Spam: So finden Sie den Absender einer E-Mail

IP-Adressen sind nicht nur ein Mittel, um Raubkopierern auf die Spur zu kommen, sondern sie können auch dabei helfen, den Absender einer E-Mail zu ermitteln. Das ist besonders für die Jagd nach einem Spammer interessant. Hilfreich ist dabei die Tatsache, dass jede E-Mail Informationen darüber enthält, welche Stationen sie durchlaufen hat und unter welcher IP-Adresse sie ihren Ursprung hat.

stop Doch Vorsicht: Wie wir im Folgenden zeigen, lassen sich sehr viele Einträge fälschen – und dadurch kann es recht schwierig werden, den wahren Urheber zu identifizieren.

Dreh- und Angelpunkt bei der Jagd nach einem Spammer sind die sogenannten Internet-Kopfzeilen (E-Mail-Header). Um an die heranzukommen, klicken Benutzer von Outlook mit der rechten Maustaste auf die E-Mail und anschließend auf *Nachrichtenoptionen*. Die Vorgehensweise bei anderen E-Mail-Clients können Sie unter der Internetadresse th-h.de/faq/headerfaq.php#mailreader finden.

Der E-Mail-Header besteht zwar lediglich aus Text, er enthält allerdings erschreckend viele Einträge – von denen die meisten für die Spammer-Jagd nur sehr am Rande interessant sind. So gibt jedes E-Mail-Programm zunächst einmal seine Identität preis. Diese Information finden Sie im E-Mail-Header unter dem Eintrag *User-Agent* einsehbar. Die Einträge *Mime-Version*, *Content-Type* und *Content-Transfer-Encoding* können Sie ebenfalls ignorieren. Sie geben lediglich Auskunft über die Codierung des E-Mail-Texts.

Der erste scheinbar wichtige Eintrag einer Spammail lautet *Return-Path*. Doch auch diesen Eintrag können Sie getrost ignorieren. In der Regel fälscht nämlich ein Spammer auch diese vermeintliche Absenderadresse. Würden Sie im E-Mail-Programm auf *Antworten* klicken, wäre das der Empfänger Ihrer Antwortmail. Besonders offensichtlich wird diese Fälschung, wenn unter *Return-Path* Ihre eigene Adresse erscheint. Vergleichen Sie den *Return-Path* mit der *Message-Id*.

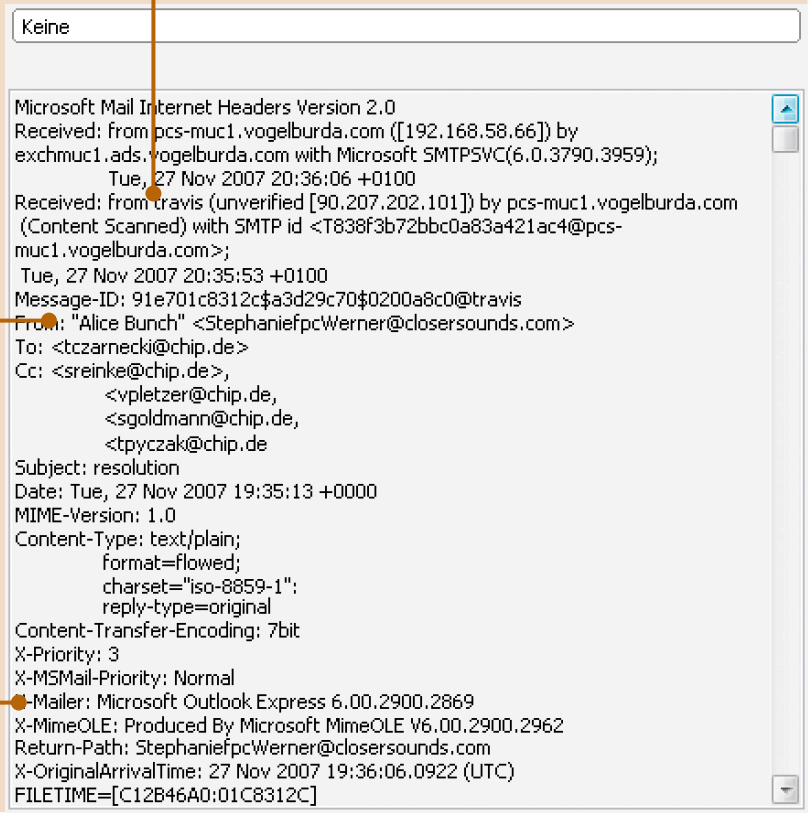
Spurensicherung in der Spammail

Jeder Spammer hinterlässt Spuren, die Sie auslesen können. Der Header, der in jeder Nachricht zu finden ist, dokumentiert den Weg der E-Mail vom Absender bis zum Empfänger. Welche Server wurden verwendet? In welcher Zeitzone stehen sie? Welche Software wurde verwendet? All das hilft, den Übeltäter zu identifizieren.

Aus dem E-Mail-Header lässt sich die Adresse des Spammer-Servers ablesen.

Die angebliche E-Mail-Adresse findet sich ebenfalls in den Internetkopfzeilen.

Selbst der Name des verwendeten E-Mail-Clients wird aufgelistet.



Diese ID ähnelt einer Trackingnummer der Post und setzt sich laut einer Regel aus einer einmaligen Zeichenkette und dem Absende-Server zusammen. Die *Message-Id* könnte also etwa *SAHDRQ@hotmail.com* lauten. Ist die vermeintliche Absende-Adresse jedoch eine Nachricht von *@yahoo.com*, wird an dieser Stelle ebenfalls der Betrugsversuch klar.

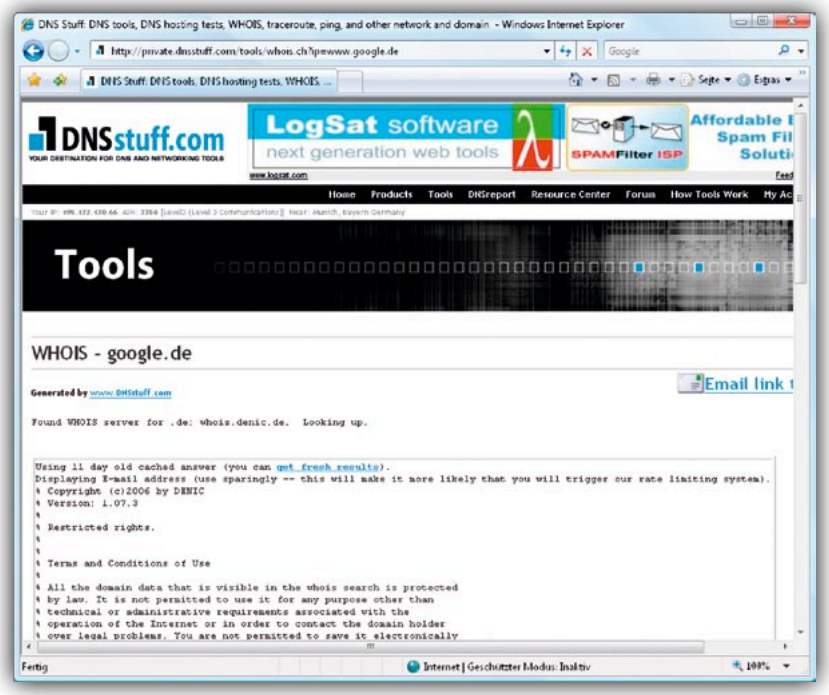
Die ersten vernünftigen Informationen bekommen Sie von den *Received*-Einträgen. An dieser Stelle können Sie nachlesen, welche Stationen die Mail durchlaufen hat. Ähnlich wie bei einem Blog ist der unterste Eintrag der älteste. Lesen sollten Sie die Einträge trotzdem von oben nach unten, da Ihr E-Mail-Server (also der oberste Eintrag) auf jeden Fall vertrauenswürdig ist. Jeder Eintrag entspricht dem Muster *Received: from X by Y with Z*. Die Absende-IP-Adresse lautet also X und wurde von Y in Empfang genommen.

Zur Übertragung wurde das E-Mail-Protokoll Z verwendet. Da jeder E-Mail-Server seinen eigenen Stil hat, sind zwar alle Einträge nach demselben Muster aufgebaut, sehen aber ansonsten vollkommen unterschiedlich aus. Lassen Sie sich davon bei Ihrer Recherche nicht abschrecken.

Das erste *by* im ersten Eintrag verrät Ihnen die Adresse Ihres E-Mail-Servers, der erste *from*-Eintrag den letzten Sender. Bei dem zweiten *Received* sollte der letzte Sender (*from*) dem zweiten *by*-Eintrag entsprechen. Doch bereits an dieser Stelle kann es abweichen-de Angaben geben. Die harmlose Ursache dafür wäre, dass der Server mehrere Adressen besitzt. Sollten sich die beiden Adressen allerdings nicht auf denselben Server zurückführen lassen, so ist der Punkt erreicht, an dem Sie sich an den Betreiber des nächsten Knotens wenden müssen. Er muss

nun über seine Serverprotokolle herausfinden, von welcher IP-Adresse die Spam-E-Mail verschickt worden ist.

Sollten Sie eine IP-Adresse als Absender identifizieren können, ermitteln Sie am besten über eine Webseite wie www.dnsstuff.com mit einer WHOIS-Abfrage, zu welchem Provider diese IP-Adresse gehört. Dort finden Sie auch eine E-Mail-Adresse, an die Sie sich wenden können. Schildern Sie Ihr Problem, und fügen Sie auch die Internetkopfzeilen in die E-Mail ein. Mit etwas Glück kann der Provider dann den Verantwortlichen ausfindig machen und das Problem lösen. Erwarten Sie allerdings nicht zu viel. Denn mittlerweile sind viele Versender von Spammails selber ein Opfer – nämlich das eines Botnetzwerks.



Info-Service: Was die IP-Adresse oder auch der Domainname alles verrät, bekommt man eindrucksvoll unter www.dnsstuff.com gezeigt.

Bots sind Rechner, die von einem Hacker kontrolliert und beispielsweise als E-Mail-Server missbraucht werden. Je mehr Bot-PCs ein Hacker unter seiner Kontrolle hat, umso mehr Spam kann er in kürzester Zeit versenden.

Da die Rechner eines Botnetzwerks zumeist kein Protokoll darüber führen, wann mit welcher IP-Adresse eine Verbindung aufgebaut wurde, endet dort die Spur, und der wahre Täter bleibt anonym.

Einzige verbleibende Chance: Beobachtet man mit Tools wie Wireshark die ein- und ausgehenden Verbindungen der Botkommunikation, findet man vielleicht die IP-Adresse der Steuerzentrale des Botnetzwerks und kann den Spammern das Handwerk legen.

Weblinks

- www.live.com
  Der Blick über den Tellerrand lohnt. Die Microsoft-Suchmaschine identifiziert über den Befehl *IP:* sämtliche Domains, die auf dem Server der angehängten IP-Adresse zu finden sind.
- www.ripe.net
  www.iana.net
  www.apnic.net
  www.lacnic.net
  Über Meldebehörden lässt sich der verantwortliche IP-Provider identifizieren.

ratschlag24.com

Das neue Ratgeber-Portal ratschlag24.com liefert Ihnen täglich die besten Ratschläge direkt auf Ihren PC.

Viele bekannte Autoren, Fachredakteure und Experten schreiben täglich zu Themen, die Sie wirklich interessieren und für Sie einen echten Nutzen bieten. Zu den Themen zählen Computer, Software, Internet, Gesundheit und Medizin, Finanzen, Ernährung, Lebenshilfe, Lernen und Weiterbildung, Reisen, Verbrauchertipps und viele mehr. Alle diese Ratschläge sind für Sie garantiert kostenlos. Testen Sie jetzt ratschlag24.com – Auf diese Ratschläge möchten Sie nie wieder verzichten.

ratschlag24.com ist ein kostenloser Ratgeber-Dienst der eload24 GmbH
www.eload24.com

Viel guter Rat ab 3 Euro monatlich
Die neuen Flatrate Modelle von eload24

Das ist ein Wort: Sie bekommen **freien Zugang zu allen eBooklets und eBooks** bei eload24. Sie können alles laden, lesen, ausdrucken, ganz wie es Ihnen beliebt. Eine echte Flatrate eben, ohne Wenn und Aber. Sie werden staunen: Unser Programm mit nützlichen eBooklet-Ratgebern ist groß und wird laufend erweitert.

Der Preisvorteil ist enorm:

24 Monate Flatrate für nur 72,– € (3,– € monatlich)

12 Monate Flatrate für nur 48,– € (4,– € monatlich)

6 Monate Flatrate für nur 36,– € (6,– € monatlich)

Selbst wenn Sie nur zwei eBooklets der preiswertesten Kategorie im Monat laden, sparen Sie im Vergleich zum Einzelkauf.

Tausende Kunden haben dieses Angebot schon wahrgenommen, profitieren auch Sie dauerhaft. Wenn Sie nach Ablauf der Flatrate weitermachen wollen, dann brauchen Sie nichts zu tun: das Flatrate-Abonnement verlängert sich automatisch. Bis Sie es beenden.

Kaufen Sie jetzt die Flatrate Ihrer Wahl. Und schon einige Augenblicke später stehen Ihnen hunderte toller Ratgeber uneingeschränkt zur Verfügung: Packen Sie mal richtig zu!

www.eload24.com/flatrate