

01010100010000100110100101110100011  
11001101110101011011100110011101100  
01010010000001100100011001010111001  
00101110100011100110010111001101110  
00110011101100101011011100010000001  
11001010111001000100000010010010101  
10111001101110011001010111010000100  
1110001000000110011011111000111001  
000100100101010000101101010100110  
10110101010011011010010110001101101

Sicher kommunizieren

Angreifer abwehren

0000110010101110010011001100110010101101011011101001  
101110110001110010100100000010000100110010101110010011  
1100101011100100110100001100101011010010111010000100  
100110011001010110101111010001100101001000000100110  
100001000010011001010111001001100101101001011000110  
0001100101011010010110100001000010000101100101010001100  
11011101000111010100100000010011011101100110011011101  
1110010011001010110100101100011011010000110101001000000  
1010000100001000010100010100001000110100101110100011  
100101010001000010011010010111010001110011001011100110111



Wertvolles schützen

- IT-Sicherheit
- Systemberatung
- Secure-Hosting

# Anleitung

## E-Mail Spam Filter mit Quarantäne

Eine kurze Funktionsübersicht

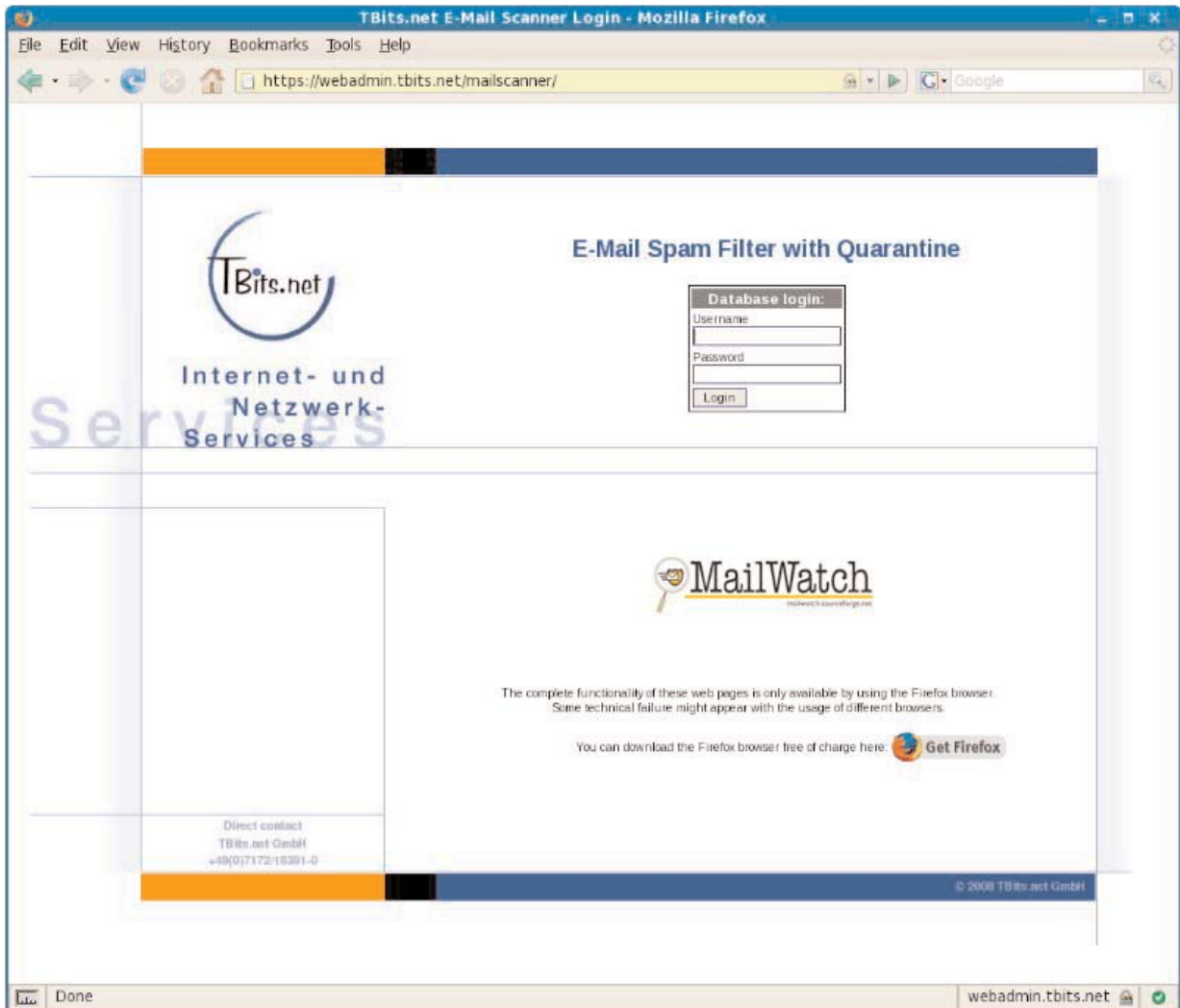


## E-Mail Spam Filter mit Quarantäne Eine kurze Funktionsübersicht

### 1. Anmeldung

Die Anmeldung erfolgt über:

<http://mailadmin.tbits.net>



Jeder Benutzer meldet sich mit der E-Mail-Adresse als Benutzername und einem Passwort an.

Wir möchten an dieser Stelle darauf hinweisen, dass der volle Funktionsumfang des E-Mail Spam Filters nur mit dem Firefox Internetbrowser zur Verfügung steht.

### TBits.net GmbH

Internet- und Netzwerk-Services

Seeweg 6 D-73553 Alfdorf  
Telefon +49 (0) 7172 18391-0  
Telefax +49 (0) 7172 18391-99  
Service +49 (0) 700 TBITSNET  
E-Mail [info@tbits.net](mailto:info@tbits.net)  
Internet [www.tbits.net](http://www.tbits.net)



## E-Mail Spam Filter mit Quarantäne Eine kurze Funktionsübersicht

### 2. Übersicht

Nach erfolgreicher Anmeldung öffnet sich die Übersicht der letzten 50 Nachrichten. Diese Übersicht aktualisiert sich automatisch alle 90 Sekunden. Benutzer sehen hier ihre gesendeten und empfangenen E-Mails.

Wenn Sie über das Recht Domänen-Administrator verfügen, sehen Sie alle E-Mails.

The screenshot displays the 'E-Mail Spam Filter with Quarantäne' web interface. At the top left is the 'TBits.net' logo. The main header includes the title 'E-Mail Spam Filter with Quarantäne' and the 'MailWatch' logo. A search bar is located below the header with the placeholder text 'Search E-Mail (\* for wildcard):'. Below the search bar is a navigation menu with tabs for 'Recent Messages', 'Lists', 'Reports', 'Tools/Links', and 'Logout'. The main content area shows a table titled 'Last 50 Messages (Refreshing every 90 seconds)'. The table has the following columns: #, Host, Date/Time, From, To, Subject, Size, SA Score, MCP Score, and Status. The table contains several rows of message data, with some rows highlighted in red to indicate spam.

#	Host	Date/Time	From	To	Subject	Size	SA Score	MCP Score	Status
[L]		24.06.08 14:34:54	info@tbits.net	info@tbits.net		1.2Kb	19.43		Spam
[L]		24.06.08 14:34:53	info@tbits.net	info@tbits.net	RE: info@tbits.net	673.5Kb		0.00	Clean
[L]		24.06.08 14:34:53	info@tbits.net	info@tbits.net		173.6Kb	-2.60		Clean
[L]		24.06.08 14:34:53	info@tbits.net	info@tbits.net		3.2Kb	27.20		Spam

Im Feld "Search E-Mail" können gezielt E-Mails mit dem Suchwort in Sender, Empfänger oder Betreff gefunden werden. Als Platzhalter kann ein \* verwendet werden.

#### Beispiele:

- info@tbits.net Sucht nach E-Mails von bzw. an "info@tbits.net".
- info\* Sucht nach E-Mails deren Sender, Empfänger oder Betreff mit "info" beginnt.
- \*tbits.net Sucht nach E-Mails, die von bzw. an die Domäne "tbits.net" gesendet wurden.
- tbits Sucht nach E-Mails, die das Wort "tbits" bei Sender, Empfänger oder Betreff enthalten.

#### Über die Menüleiste gelangen Sie zu folgenden Bereichen:

<b>Recent Messages</b>	Übersicht der letzten 50 Nachrichten. Hierüber gelangen Sie auch in die Detailansicht von Nachrichten, in der u. a. E-Mails aus der Quarantäne freigegeben oder gelöscht werden können.
<b>Lists</b>	Pflege der Black- und Whitelisten.
<b>Reports</b>	Auswertungen mit weiteren Filtermöglichkeiten.
<b>Tools/Links</b>	Benutzerverwaltung. Dieser Menüpunkt steht Ihnen nur als Domänen-Administrator zur Verfügung.
<b>Logout</b>	Aus dem E-Mail Spam Filter abmelden.

### TBits.net GmbH

Internet- und Netzwerk-Services

Seeweg 6 D-73553 Alfdorf  
 Telefon +49 (0) 7172 18391-0  
 Telefax +49 (0) 7172 18391-99  
 Service +49 (0) 700 TBITSNET  
 E-Mail info@tbits.net  
 Internet www.tbits.net



# E-Mail Spam Filter mit Quarantäne

## Eine kurze Funktionsübersicht

### 3. Recent Messages

#### Übersicht letzte 50 Nachrichten

In dieser Übersicht sehen Sie die letzten 50 Nachrichten. Hier werden Datum sowie weitere Kurzinformationen zu den Nachrichten angezeigt. Die Einstufung der E-Mail zeigt die farblich hinterlegte Zeile. Eine Legende mit Erläuterungen finden Sie oben auf der Seite im Kasten "Color Codes".

Um in die Detailansicht einer Nachricht zu gelangen, klicken Sie in das Feld [ ] in der ersten Spalte. Es öffnet sich die Detailansicht, wo auch weitere Aktionen für die E-Mail (freigeben, löschen, weiterleiten, black/whitelisting) durchgeführt werden können.

### 4. Nachrichtendetails

#### Detailansicht mit Aktionen

Diese Ansicht gibt Auskunft über die Einzelheiten einer E-Mail. Über die Links "Add to Whitelist" / "Add to Blacklist" können der Absender (Feld "From:") oder sendende Rechner (Feld "Received from:") in eine der beiden Listen aufgenommen werden.

Neben den Kopfdaten (sog. Header) der E-Mail werden auch weitere Informationen zur Einstufung der E-Mail angezeigt.

The screenshot displays the MailWatch interface for an email message. At the top, there are logos for TBits.net and MailWatch, along with a search bar. A 'Color Codes' legend and 'Today's Totals' table are also visible. The main content area shows the message details:

Received on:	24.06.08 16:21:35
Received by:	mailgate01
Received from:	89.105.159.35
Received Via:	IP Address: 89.105.159.35, Hostname: (Reverse Lookup Failed), Country: Russian Federation, RBL: [ ], Spam: [ ], Virus: [ ], All: [ ]
ID:	m50EKwma001839

**Message Headers:**

Return-Path: <A@g>  
Received: from unipr.it (89.105.159.35) by smailgate01.tbits.net (8.13.66.13.8) with SMTP id m50EKwma001839 for <[redacted]>; Tue, 24 Jun 2008 16:20:59 +0200  
Return-Path: <[redacted]>  
Received: from 83.245.63.64 (HELO [redacted]) by emode with esmtp (fnChar[8-12]) (fnChar[4-6]) id CB21XE-Use1Kd-rK for [redacted]@[redacted]; Tue, 24 Jun 2008 22:21:05 +0800  
Message-ID: <019701c8d1605889d690a08c0a800e2@Mac>  
From: "[redacted]" <[redacted]>  
To: [redacted]  
Subject: High quality for low price  
Date: Tue, 24 Jun 2008 22:21:05 +0800  
MIME-Version: 1.0  
Content-Type: multipart/alternative; boundary="-----\_NextPart\_05\_01FF\_01C8D64897F9D0A7"  
X-Priority: 3  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook Express 6.00.2800.1158  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2800.1158

From: [redacted] [Add to Whitelist | Add to Blacklist]  
To: [redacted]  
Subject: High quality for low price  
Size: 2.8kb

Anti-Virus/Dangerous Content Protection  
Virus: N

TBits.net GmbH  
Internet- und Netzwerk-Services

Seeweg 6 D-73553 Alfdorf  
Telefon +49 (0) 7172 18391-0  
Telefax +49 (0) 7172 18391-99  
Service +49 (0) 700 TBITSNET  
E-Mail info@tbits.net  
Internet www.tbits.net



## E-Mail Spam Filter mit Quarantäne Eine kurze Funktionsübersicht

Der Betreff einer E-Mail wird um Stichworte ergänzt, wenn der Inhalt vom Quarantäne-Filter verändert wird. Steht im Betreff z. B. {Disarmed}, so wurden in eine HTML-Mail eingebettete Objekte (z. B. Flash-Animationen) herausgefiltert.

Wurde eine Nachricht in Quarantäne genommen, so befindet sich ganz unten auf der Seite der Block **“Quarantine”**.

Release	Delete	SA Learn	File	Type	Path	Dangerous?
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/> As Ham	message	message/rf822	var/spool/MailScanner/quarantine/20080624/spam/m50FKwma001839	<input checked="" type="checkbox"/>

Über die Funktion **Release** kann die E-Mail bzw. einzelne Teile der E-Mail aus der Quarantäne freigegeben und an den Empfänger weitergeleitet werden.

**“Alternate Recipients:”** sendet die E-Mail an alternative Empfänger.

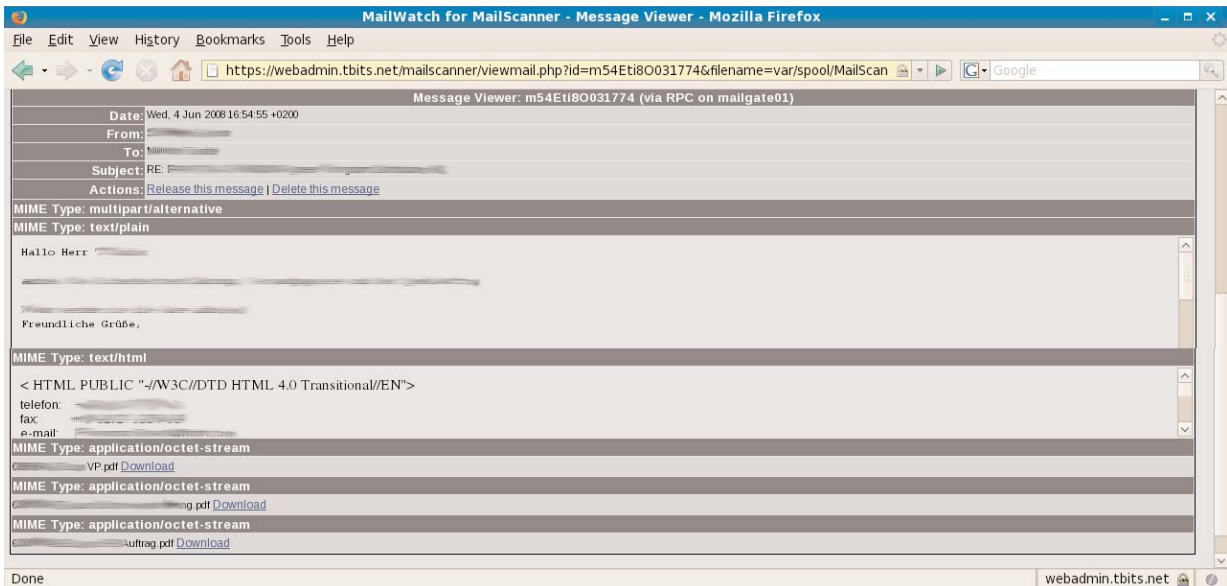
**“Delete”** löscht die E-Mail vom Server. Der Eintrag wird jedoch weiterhin in der Liste angezeigt. Erst nach 30 Tagen wird der Eintrag permanent aus der Liste entfernt.

Die Funktion **“SA Learn”** trainiert den E-Mail Filter mit der gewählten Aktion.

Ein Klick auf den Button **“Submit”** führt die gewählten Aktionen aus.

## E-Mail Spam Filter mit Quarantäne Eine kurze Funktionsübersicht

Handelt es sich bei dem angezeigten Listeneintrag um den Nachrichteninhalt, so kann die Nachricht über den Link in der Spalte **“Path”** angezeigt werden:



In der Nachrichteninhaltsansicht kann die Nachricht dann ebenfalls freigegeben oder gelöscht werden. Sind Dateianhänge in der E-Mail, so können diese über den Link **“Download”** am Seitenende heruntergeladen werden.

### 5. Lists

#### Verwalten von Black- und Whitelisten

In der Whitelist wird angegeben, welche E-Mails immer zugestellt werden sollen. Die Blacklist beinhaltet Einträge für nicht erwünschte E-Mails. Der Benutzer kann hier die eigenen Einträge verwalten. Ein Domänen-Administrator kann für die Domäne gültigen Einträge sowie die Einträge der Benutzer verwalten.

Das Anlegen von neuen Einträgen erfolgt über die Links **“Add to Whitelist / Blacklist”**. Im Feld **“From:”** kann eine E-Mail Adresse, Domäne oder die IP-Adresse eines Rechners eingetragen werden. Das Feld **“To:”** gibt an, ob das Ziel eine bestimmte E-Mail Adresse oder für die gesamte Domain gültig ist. Sollen alle Einträge für eine bestimmte Adresse gültig sein, so kann das Schlüsselwort **“default”** verwendet werden.

Das Löschen eines Eintrags wird mit einem Klick auf den dahinterstehenden Link **“Delete”** durchgeführt.

TBits.net GmbH

Internet- und Netzwerk-Services

Seeweg 6 D-73553 Alfdorf  
Telefon +49 (0) 7172 18391-0  
Telefax +49 (0) 7172 18391-99  
Service +49 (0) 700 TBITSNET  
E-Mail info@tbits.net  
Internet www.tbits.net



## E-Mail Spam Filter mit Quarantäne Eine kurze Funktionsübersicht

### 6. Reports

#### Filtermöglichkeiten und Auswertungen

Diese Ansicht bietet die Möglichkeit, eine Vielzahl von Filtern für Nachrichten anzuwenden und zu speichern. Ein aktiver Filter wird im Block **“Active Filters”** angezeigt. **“Add Filter”** bietet die Auswahl an Möglichkeiten, einen oder mehrere Filterkriterien zu erstellen. Häufig benötigte Filter können über **“Save”** gespeichert werden.

The screenshot displays the MailWatch web interface. At the top left is the TBits.net logo. The main header reads "E-Mail Spam Filter with Quarantine" and "MailWatch" with the tagline "mailwatch.sourceforge.net". A search bar is present with the text "Search E-Mail (\* for wildcard):".

On the right side, there are two summary tables:

Color Codes		
Bad	Red	
Content/Infected	Orange	
Spam	Yellow	
High Spam	Light Green	
MCP	Green	
High MCP	Dark Green	
Whitelisted	Light Blue	
Blacklisted	Dark Blue	
Clean	White	

Today's Totals		
Processed:	20,767	1.5Gb
Clean:	7,471	36.0%
Viruses:	43	0.2%
Top Virus:		None
Blocked files:	62	0.3%
Others:	3	0.0%
Spam:	1,116	5.4%
High Scoring Spam:	12,072	58.1%
MCP:	0	0.0%
High Scoring MCP:	0	0.0%

Below these tables is a navigation menu with tabs for "Recent Messages", "Lists", "Reports", "Tools/Links", and "Logout".

The main content area is divided into several sections:

- Active Filters:** Shows two active filters: "From Domain contains 'tbits.net'" and "Date is greater than '2008-06-01'". Each has a "Remove" link.
- Add Filter:** A form with a "Date" dropdown, a "is equal to" dropdown, and an "Add" button.
- Load/Save Filter:** A form with a dropdown menu (set to "None") and "Load", "Save", and "Delete" buttons.
- Statistics (Filtered):** Shows "Oldest record: 02.06.08", "Newest record: 24.06.08", and "Message count: 290".
- Reports:** A list of report links: Message Listing, Message Operations, Total Messages by Date, Top Mail Relays, Top Viruses, Virus Report, Top Senders by Quantity, Top Senders by Volume, Top Recipients by Quantity, Top Recipients by Volume, Top Sender Domains by Quantity, and Top Sender Domains by Volume.

Die aktiven Filter werden beim Aufruf eines unten stehenden Reports angewendet.

So werden beim Report **“Message Listing”** im obigen Beispiel alle Nachrichten angezeigt, die nach dem 01.06.2008 an die Domäne “tbits.net” gesendet wurden. Es stehen viele weitere grafische Auswertungsmöglichkeiten in der Liste zur Verfügung.

TBits.net GmbH

Internet- und Netzwerk-Services

Seeweg 6 D-73553 Alfdorf  
Telefon +49 (0) 7172 18391-0  
Telefax +49 (0) 7172 18391-99  
Service +49 (0) 700 TBITSNET  
E-Mail info@tbits.net  
Internet www.tbits.net



## E-Mail Spam Filter mit Quarantäne Eine kurze Funktionsübersicht

### 5. Tools / Links

#### Benutzerverwaltung

Dieser Menüpunkt steht Domänen-Administratoren zur Verfügung.

Unter dem Punkt **“Usermanagement”** können alle Zugänge zum E-Mail Spam Filter für eine Domäne verwaltet werden.

Der Benutzername entspricht der E-Mail Adresse. Ebenfalls verwaltet werden können z. B. Name, Passwort und Berechtigung des Benutzers. Optional kann täglich ein Bericht per E-Mail versendet werden, der über die Quarantäne E-Mails informiert.

### 6. Logout

#### Vom E-Mail Spam Filter abmelden

Beenden Sie Ihre Sitzung über den Menüpunkt **“Logout”**. So können Sie sicherstellen, dass Unberechtigte keinen Zutritt zu Ihren E-Mails erhalten.