



Ethical Hacking and Countermeasures

Version 6



Module XL

Spamming

nzherald.co.nz

'Celebrity Gang' behind 23% of all spam

12:07PM Thursday November 29, 2007

By [Matt Greenop](#)

A group of spammers, with a fondness for using celebrity names in its spam, is now controlling a network of compromised computers large enough to rival the massive 'Storm Worm' botnet.

A botnet is a network of computers that are under the control of hackers, usually with the rightful owner blissfully unaware that their machines have been hijacked.

Botnets, with their massive computing power, are used to distribute vast amounts of spam by email that usually contains malware that will allow the cyber crooks to steal personal information like passwords.

If not caught, the spammer's botnet networks will grow exponentially.

The group is now responsible for more than 20 per cent of all spam in circulation, according to New Zealand-based internet security specialist Marshal.

The Celebrity Gang, which uses subject lines about nude celebrities like Angelina Jolie and Britney Spears, has been building its botnet since August 2006.

Other subject lines that the gang use to deliver malware to computers include Windows Security Updates and promises of free games.

Source: <http://www.nzherald.co.nz/>

Module Objective

This module will familiarize you with:

Spamming

Techniques used by Spammers

How Spamming is performed

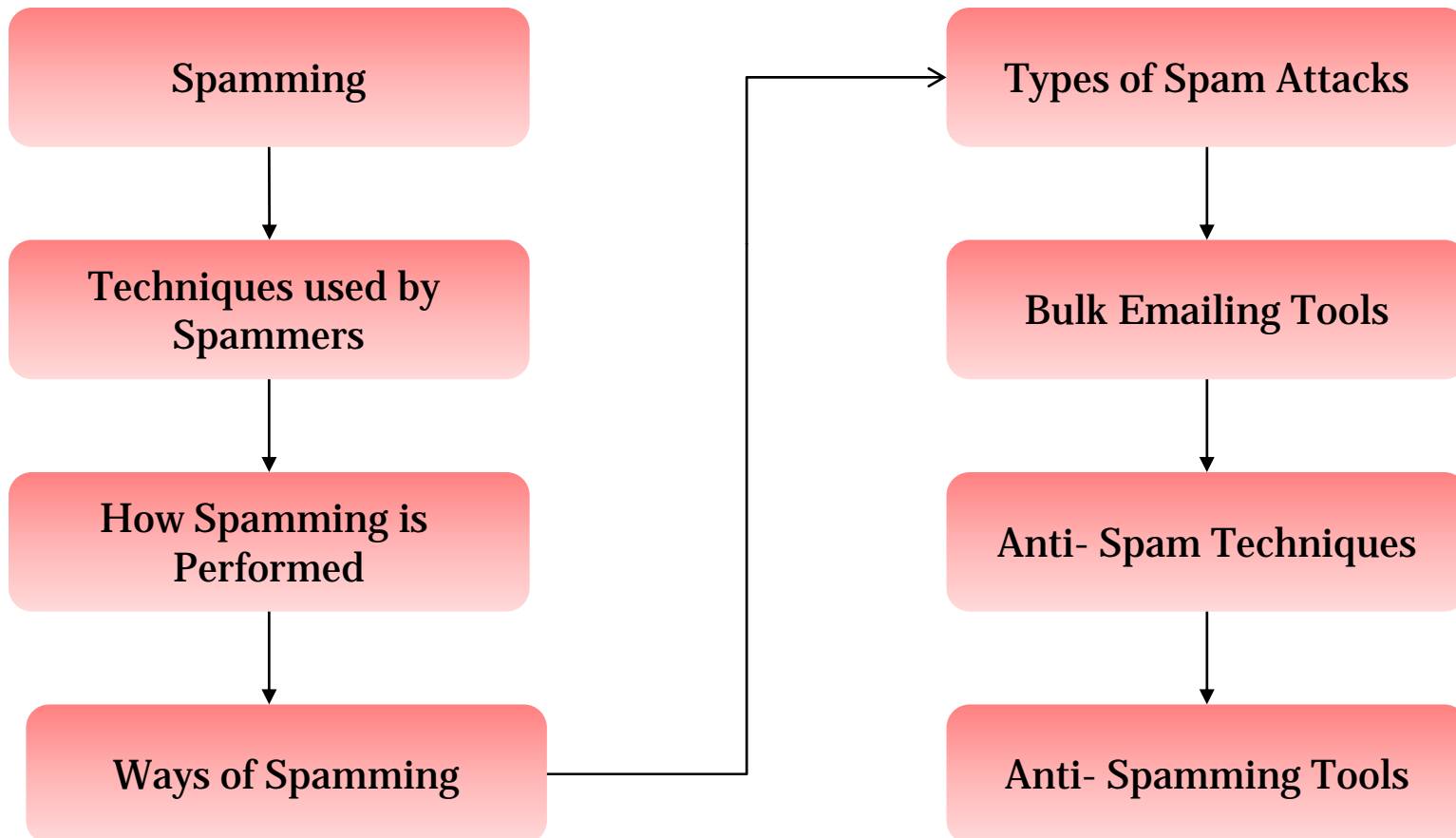
Ways of Spamming

Types of Spam attacks

Bulk Emailing Tools

Anti-Spam Techniques

Anti- Spamming Tools



Introduction

Spamming is populating the user's inbox with unsolicited or junk emails

Spam email contains malicious computer programs such as viruses and Trojans which change the computer settings or track the system

Spamming is also used for product advertisements



Techniques Used by Spammers

Spoofing the domain:

- Message appears to be from user's own domain

Poisoning or spoofing filters:

- Addition of invisible text or numbering in message

Social Engineering:

- Used to manipulate people to perform actions or divulge confidential information

Directory harvesting:

- By sending messages to possible addresses and then building a list of valid email addresses through non-delivery reports

Phishing attacks:

- Convinces the user that the mail is sent by a trusted source

Techniques Used by Spammers (cont'd)

Sending virus attached files:

- It installs Trojan horse and viruses that malfunction host computer

Database Poisoning:

- Using innocuous words (ham words) in a SPAM, thereby effectively poisoning the database in the long run

Junk Tags:

- Hiding spam words by inserting invalid HTML tags in between words

Invalid Words:

- Spam word like mortgage etc. are masked by inserting special characters or junk characters in between

How Spamming is Performed

Getting the email ID's

- Spammers get access to the email ID's when the user registers to any email service, forums, or blogs by hacking the information or registering as genuine users
- Spiders are used which searches the code in web pages that looks as email ID's and copies it to the database
- E-mail extraction tools that have built in search engines to find email ID's of companies based on the key words entered are used
- On-line Ad Tracking tools help the spammers to analyze details of the number of users who opened the spam mails, the responses to it, and which ad brought the best results



How Spamming is Performed (cont'd)

How Spam is Relayed

- Rogue ISPs obtain their own network numbering and multiple domain names from the interNIC using which spammers manage to get across spam blocks
- On-the-fly Spammers - Spammers register as genuine users for trial accounts with ISPs and use forged identities to start spam hits
- Blind Relayers – Some servers relay a message without authentication which is sent as genuine mail



Getting passed the anti spam softwares

- The subject line of the email is given as 'Re: or Fw:' assures the anti spam softwares that it is a genuine reply to users message
- The spam message is enclosed as an image in the mail to make the anti spam software trust the source



Ways of Spamming

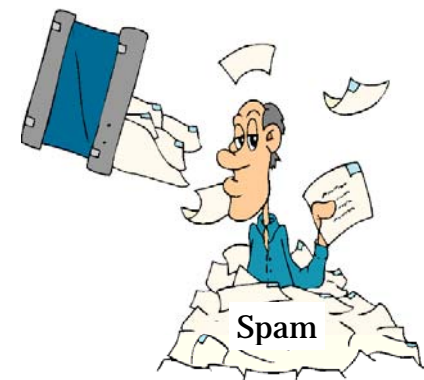
Usenet spam

- It is a single message sent to 20 or more Usenet newsgroups
- It robs users of the newsgroups by overwhelming them with a barrage of advertising or other irrelevant posts



Email Spam






- Email spam targets individual users with direct mail messages
- Email spam lists are often created by scanning Usenet postings, stealing Internet mailing lists, or searching the Web for addresses



Spammer: Statistics

The 10 Worst ROKSO Spammers

As at
26 February 2008

Rank	Photo	Spammer or Spam Gang	Country
1		Leo Kuvayev / BadCow Russian/American spammer. Does "OEM CD" pirated software spam, copy-cat pharmaceuticals, porn spam, porn payment collection, etc. Spams using virus-created botnets and seems to be involved in virus distribution. Partnered with Vlad - aka "Mr. Green"	Russian Federation
2		Alex Blood / Alexander Mosh / AlekseyB / Alex Polyakov So many Alex & Alexey spamming! Alex Blood tied to Pilot Holding & bbasafehosting.com long ago, then Alex Polyakov posted he owned them. Massive botnet and child-porn spam ring, also pharma, mortgage, and more. May work with Kuvayev and Yambo.	Ukraine
3		Vincent Chan / yoric.net Vincent Chan and his Chinese partners have been sending spam for years. They mainly do pharmacy, and are able to send out huge amounts daily. They use a vast amount of compromised machines, for sending, hosting and proxyhijacking.	Hong Kong
4		Russian Business Network Among the world's worst spammer, child-pornography, malware, phishing and cybercrime hosting networks. Provides "bulletproof hosting", but is probably involved in the crime too.	Russian Federation
5		Nikhil Kumar Pragji / Dark-Mailer Through the Dark-Mailer Windows based proxy-botnet based spamware, this spammer is responsible for and behind a large portion of the world's illegally sent spam.	Australia Queensland

Source: <http://www.spamhaus.org/>

Worsen ISP: Statistics

The 10 Worst Spam Service ISPs		As at 26 February 2008
Rank	Network	Number of Current Known Spam Issues
1	ttnet.net.tr	40
2	hinet.net	35
3	calpop.com	31
4	vsnlinternational.com	29
5	zbyd	29
6	xo.com	28
7	iplan.com.ar	28
8	casablanca.cz	28
9	internap.com	27
10	gilat.net	26

Source: <http://www.spamhaus.org/>

Top Spam Effected Countries: Statistics

The 10 Worst Spam Origin Countries		As at 26 February 2008
Rank	Country	Number of Current Known Spam Issues
1	United States	<u>1600</u>
2	China	<u>455</u>
3	Russian Federation	<u>274</u>
4	United Kingdom	<u>201</u>
5	South Korea	<u>180</u>
6	Germany	<u>173</u>
7	Japan	<u>155</u>
8	France	<u>145</u>
9	Canada	<u>131</u>
10	Taiwan	<u>124</u>

Source: <http://www.spamhaus.org/>

Types of Spam Attacks

Hidden text & links

- Making the text look same as the back ground color

Double tags

- Giving duplicate title tags and Meta tags

Cloaking

- This is done by showing different pages to search engine and users

Blog & Wiki spamming

- Wiki's are used to add or update the content of any page on the website
- This spamming allows the spammers to automatically run crawlers which hunt out blogs and then post keyword text links

Types of Spam Attacks (cont'd)

Image Spam

- In this type of spamming, emails containing only images without any text are sent by spammers to evade security systems/controls

Hijacking/pagejacking

- Redirecting a page which improves the page rank of the redirected page



Spam



Bulk Emailing Tools

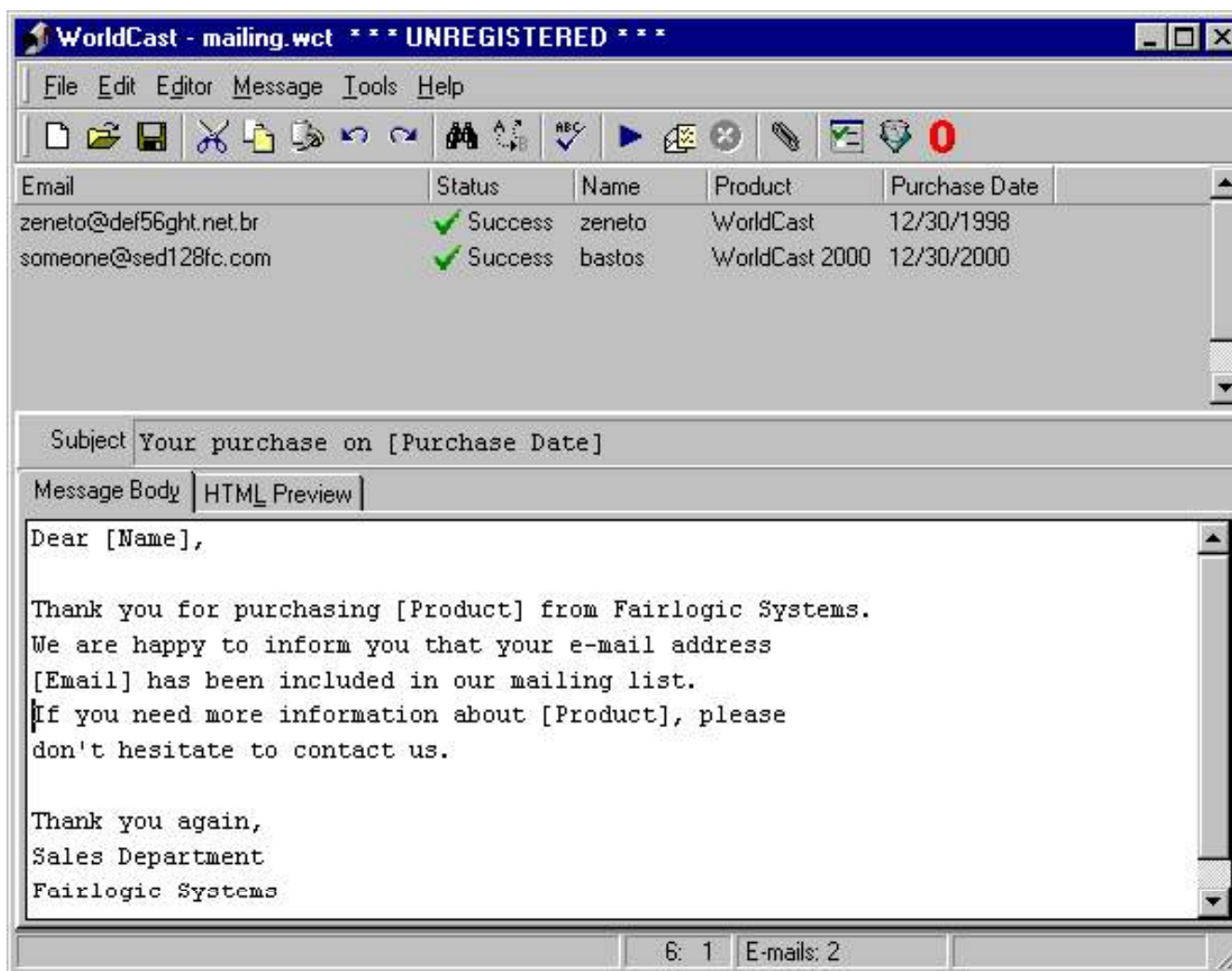
Fairlogic Worldcast bulk emailing tool is a customized mailer and also an address validator

It detects many common bad addresses existing on the mailing lists

It provides a detailed logs of the entire delivering process and reports if there is any kind of error



Fairlogic Worldcast: Screenshot



123 Hidden Sender

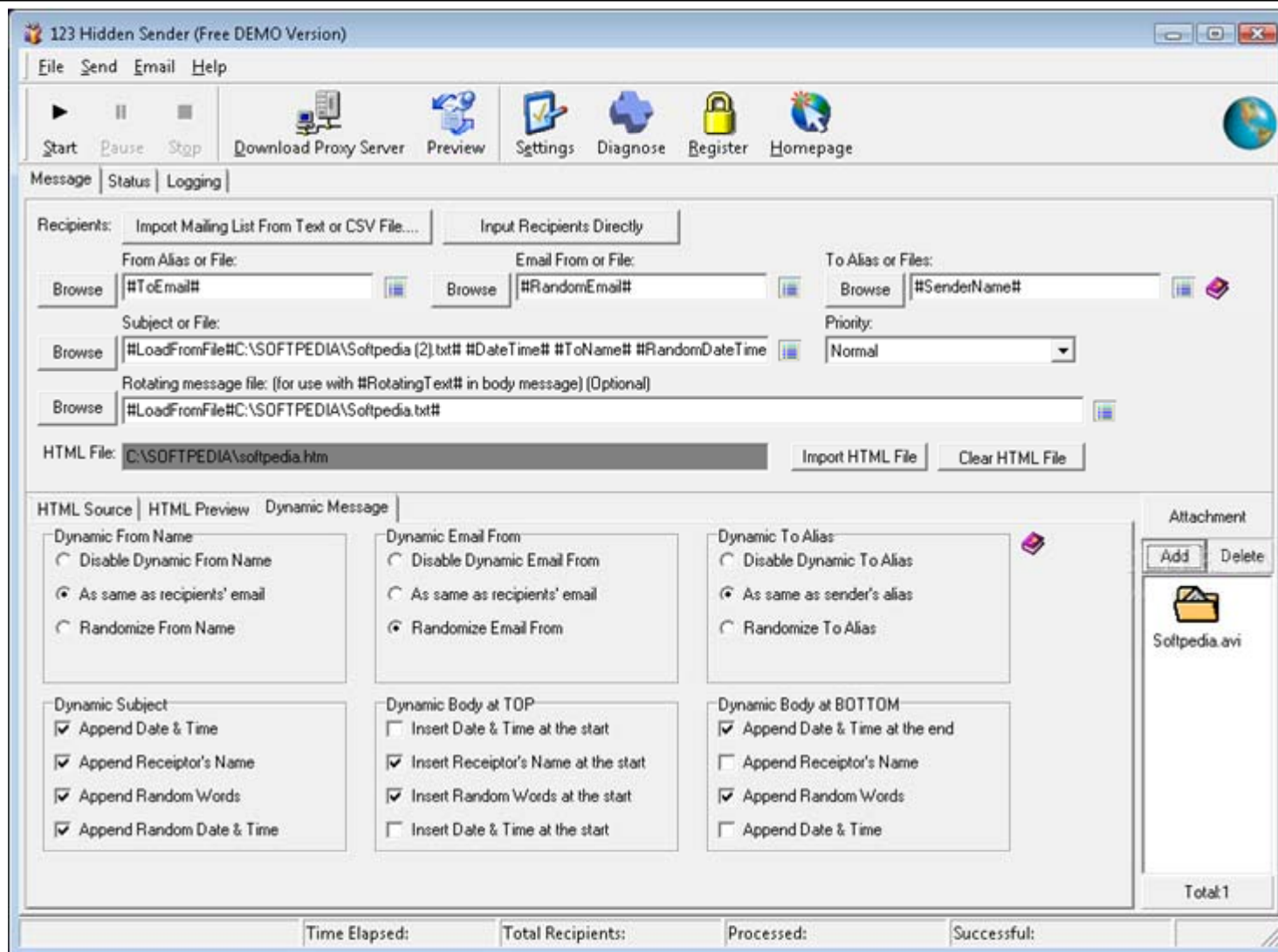
123 Hidden Sender sends absolute anonymous bulk emails

The IP address is not shown in the email headers

ISP service is not lost



123 Hidden Sender: Screenshot



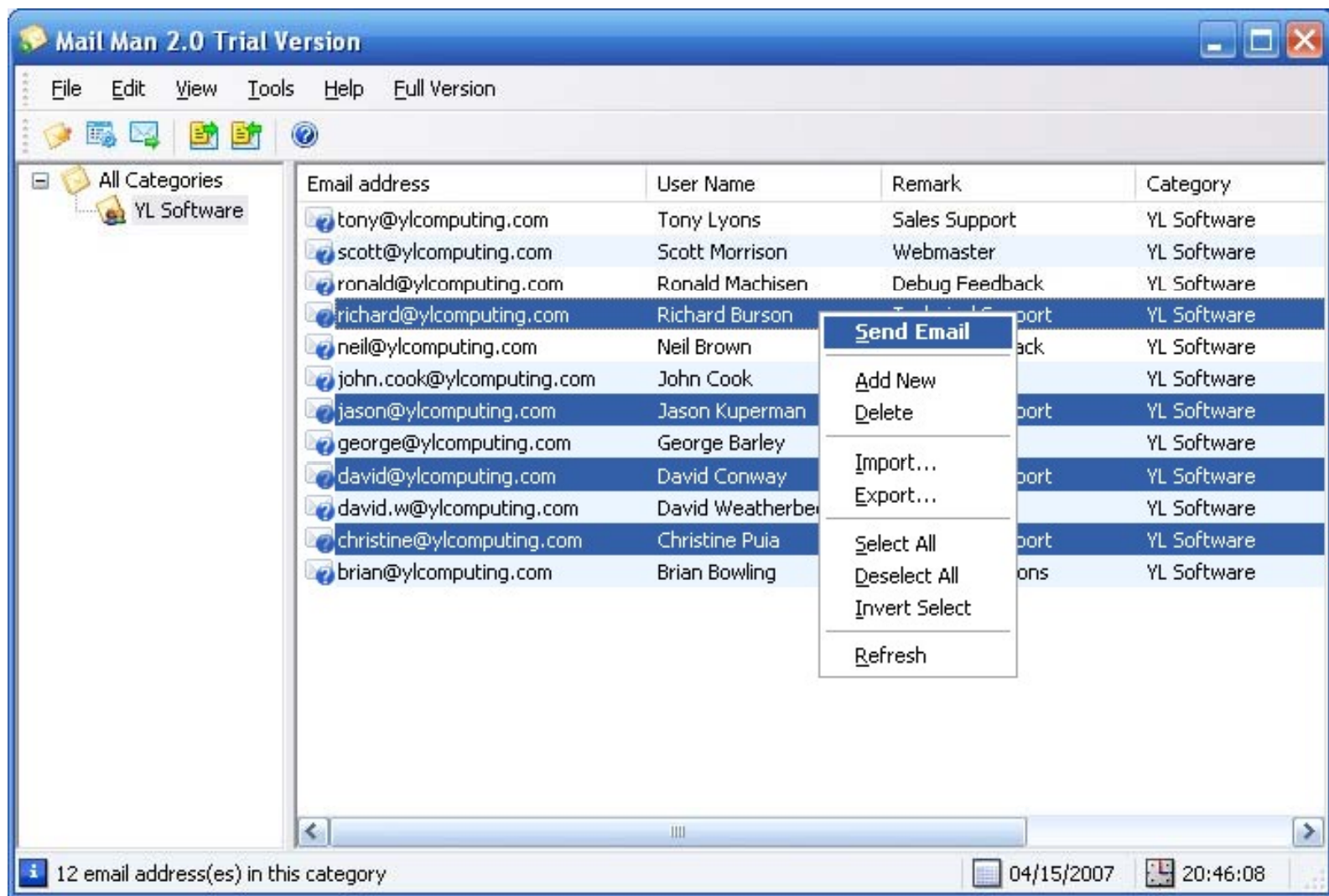
YL Mail Man is a flexible email addresses management and email delivering software

It helps companies or shareware authors to organize and manage large volumes of customer email addresses and contact them by email in simple steps

It also has import & export function and a duplicate email addresses remover



YL Mail Man: Screenshot



Sendblaster

Bulk email software for email marketing, which allows to communicate with customers and friends

It creates and sends customized e-mails using the spammers database and integrating with the web site mailing list



Sendblaster: Screenshot



Direct Sender allows to quickly and easily send unlimited numbers of personalized e-mail messages using any kind of database

The bulk process sends upto 100 simultaneous emails directly to recipients

Millions of customized emails in HTML or plain format can be send, with or without attachments and without overloading ISP's servers



Direct Sender: Screenshot

DirectSender

EMAILS parameters

Your name: yarek chmielewski Your email: yarek.c@yahoo.fr
DNS Server: 195.242.64.67 Emails packets: 5 Attachments:

Name	email
yarek	yarek.c@proxymis.fr
alvaro	alvaro@sanabria.as
Olga	Olgaesthers@yahoo.com
Proxymis	yarek@proxymis.com
jasanab	jasanab2000@yahoo.com
dialogoo	webmaster@dialogoo.com

Email Subject: hello <= Name => ☒ HTML Format

```
<html>
<body>
<b>Hello <= Name =>/b>
here comes your newsletter <b>n#6</b>
```

Message Preview 1 / 7 Sent to: (c) Proxymis

Hotmailer is a bulk email sender, email address finder, and verifier

It can efficiently search large amount of e-mail addresses from a mail server in a short time

With built in SMTP server, it will connect to the remote server and post email addresses for verification

If the email address is valid, Hotmailer will automatically send the mail



PackPal Bulk Email Server

PackPal Bulk Email Server is a safe and fast bulk email sender

It can run as a background service

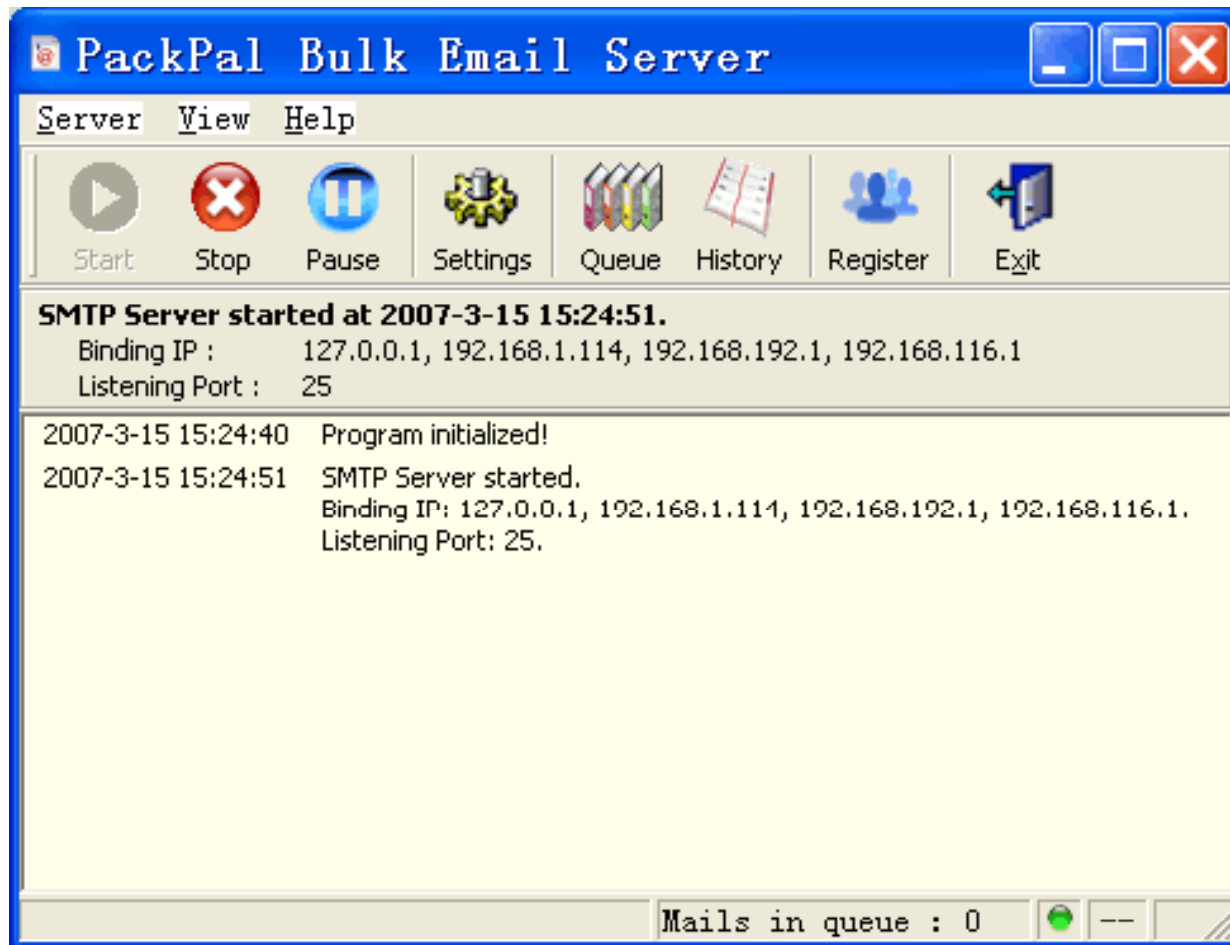
It can work with most mail clients

Features:

- Super Bulk Email Marketing tool
- The way to promote web presence
- There is no limit on the amount of messages send through the bulk email server



PackPal Bulk Email Server: Screenshot

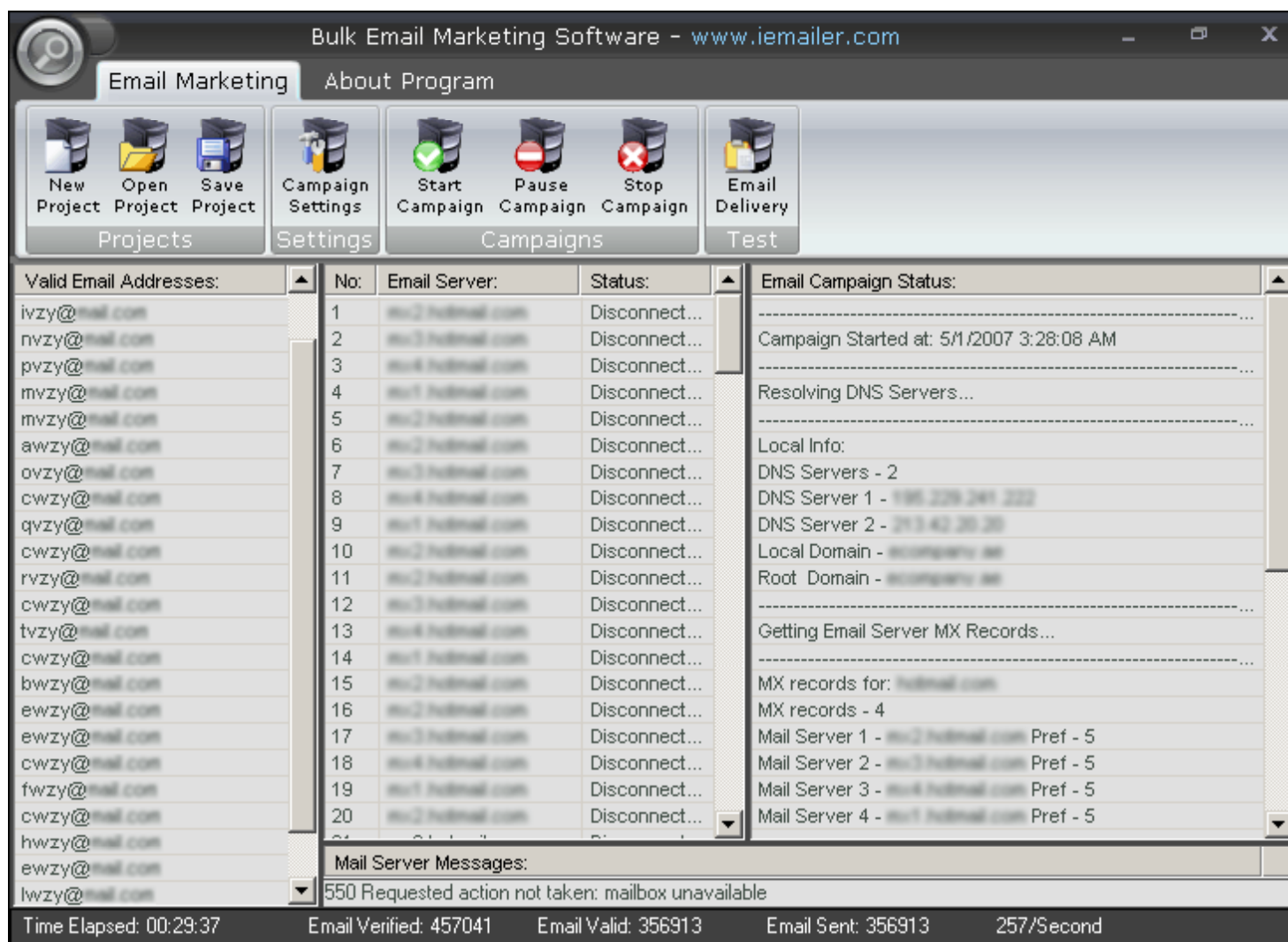


IEmailer is a bulk email marketing software which is safe to use since it does not use or go through the local ISPs email server

It simulates the sending of the email messages to the server you choose, the same one you are verifying email addresses on



IEmailer: Screenshot





Anti-Spam Techniques

Anti-Spam Techniques

Techniques used to eliminate spam are:

Heuristic/Signature-based Content Filtering

- Messages received are checked to match certain patterns
- Scores are assigned based on the patterns and if the score is higher, then the email is an undesired email

Bayesian Content Filtering

- It filters and sorts the emails into different folders based on the good and undesired mail feed to it

Collaborative Content Filtering

- Many users share their judgment about what is a desired mail and undesired mail
- Every time the user receives a mail, a special application suggest whether it is SPAM or not

Anti-Spam Techniques (cont'd)

Black Listing (RBL)

- It uses various spam detection tools, to report bad-behavior IP address as a list
- The information is collected and stored in a database to filter the spam email based on this information

White Listing

- It accepts all the emails from certain IP addresses
- No other filters can stop an email once it is accepted

Greylisting

- It does not accept the messages from IP address which are not previously successfully connected to the mail server

Anti-Spam Techniques (cont'd)

Sender Policy Framework

- To prevent the sender address forgery, SPF proposes valid email sender register i.e. the IPs of the machines they send email from, using extended DNS records

DNS-based Block Lists

- It is used to add the spam IP addresses to a local block list

MX Callbacks

- It supports callbacks which verifies the sender of a message with their MX server

Teergrubing

- It responds slowly to connected mail servers by using multi line SMTP responses



Anti-Spam Techniques (cont'd)

Reputation Control

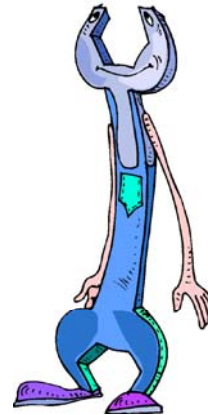
- It analyzes the email sent by the sender and assigns a score
- If the email is found to be legitimate - score improves, if not - the score reduces



Transparent SMTP Proxy

- This software blocks SMTP sessions used by e-mail worms and viruses on the NA(P)T router
- It acts like proxy, intercepting outgoing SMTP connections and scanning session data on-the-fly





Anti-Spamming Tools

AEVITA Stop SPAM Email

AEVITA Stop SPAM Email helps to hide email addresses from spambots

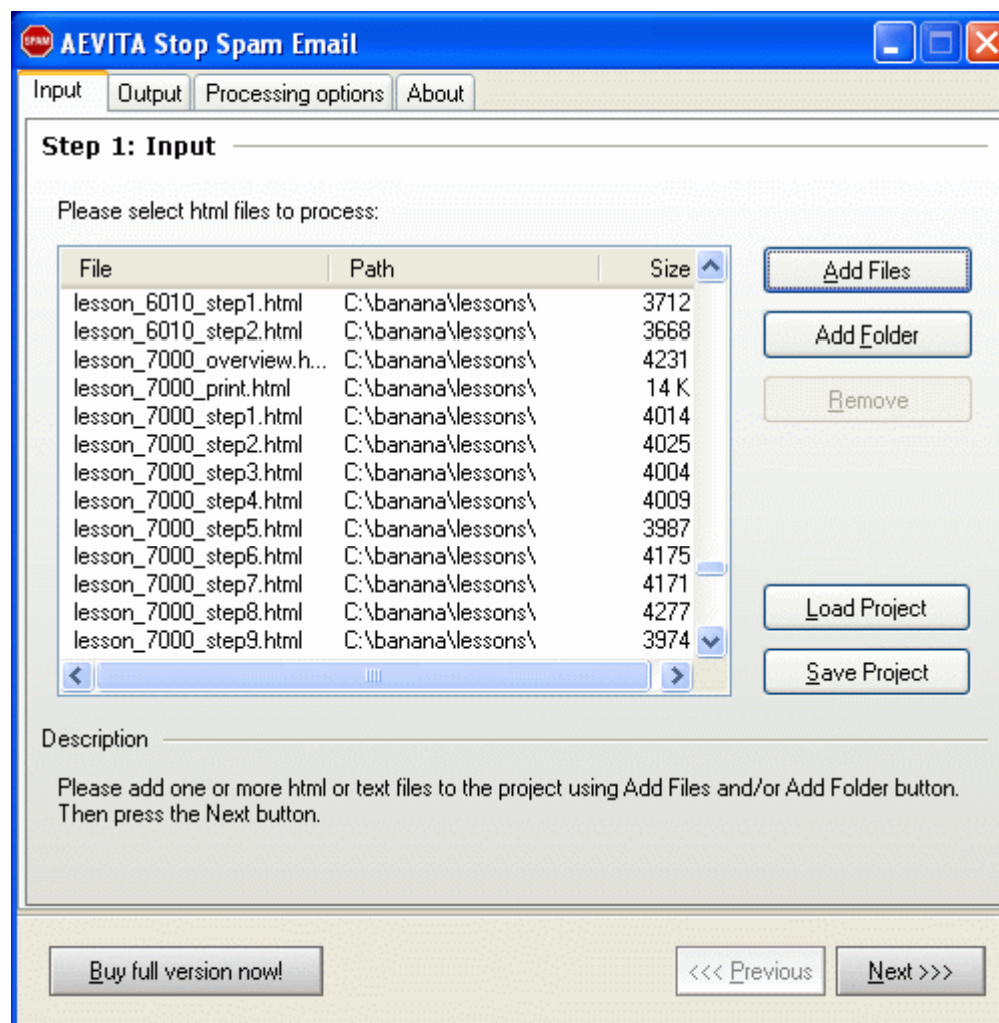
It will replace all the email addresses on the page with specifically encoded email addresses

It introduces codes that spambots block, which a normal mailing program ignores

It even stops spammers from getting a large list of email addresses



AEVITA Stop SPAM Email: Screenshot



SpamExperts Desktop

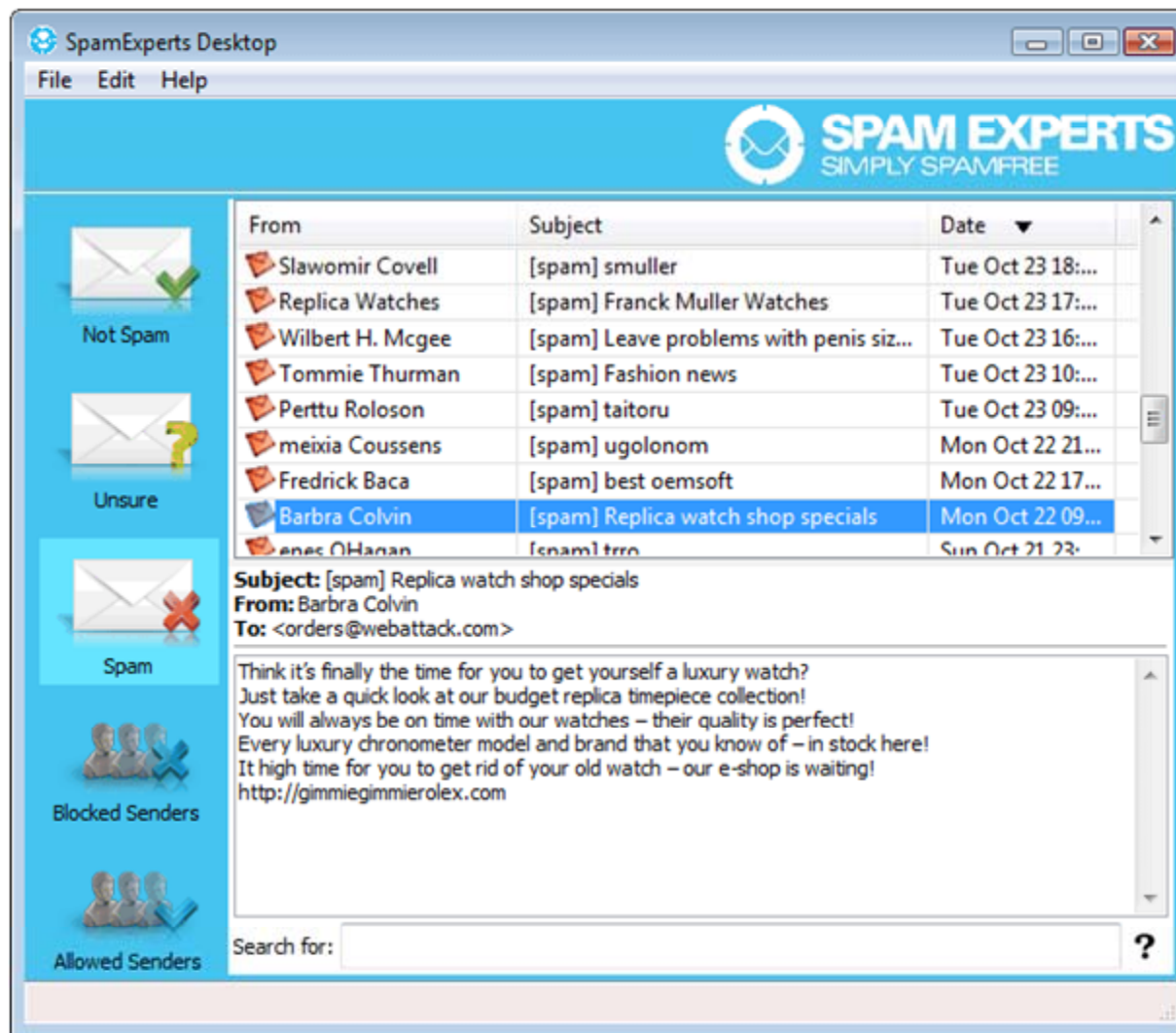
SpamExperts Desktop works as a spam filter with any email program and automatically intercepts spam

It is not dependent on keywords list to detect spam, but checks the content of message whether accepted or rejected from user

It also checks for filtering spam in background, and also maintains list of blocked and accepted senders



SpamExperts Desktop: Screenshot



SpamEater Pro is an anti-spam and email notification system

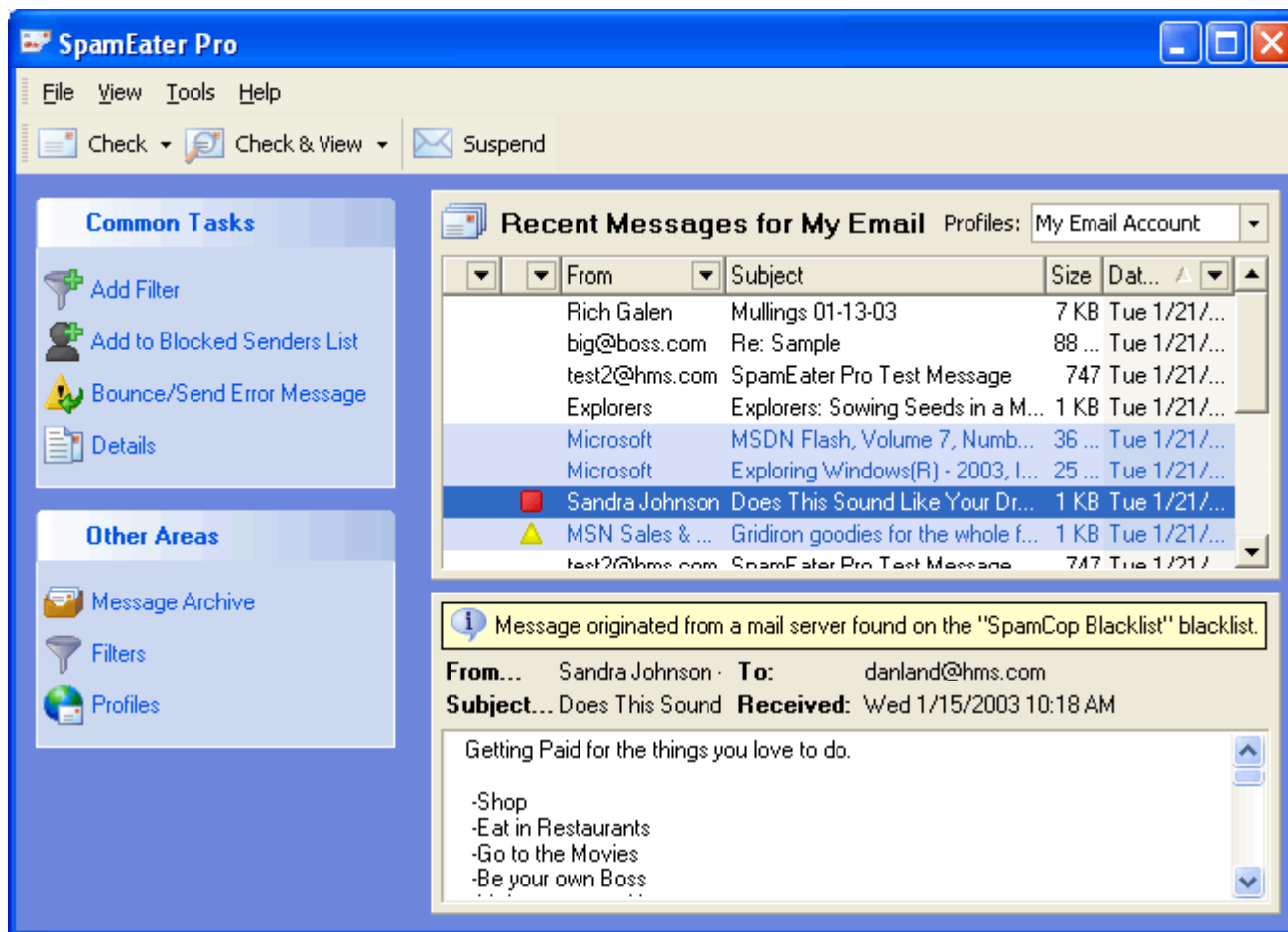
It reduces the spam in the mailbox by 95 percent

SpamEater Pro notifies the waiting mails after clearing the spam using a popup window

It provides complex rule processing, a POP3 Profile Wizard, a Rules Wizard, and support for real-time Blacklist database lookups



SpamEater Pro: Screenshot



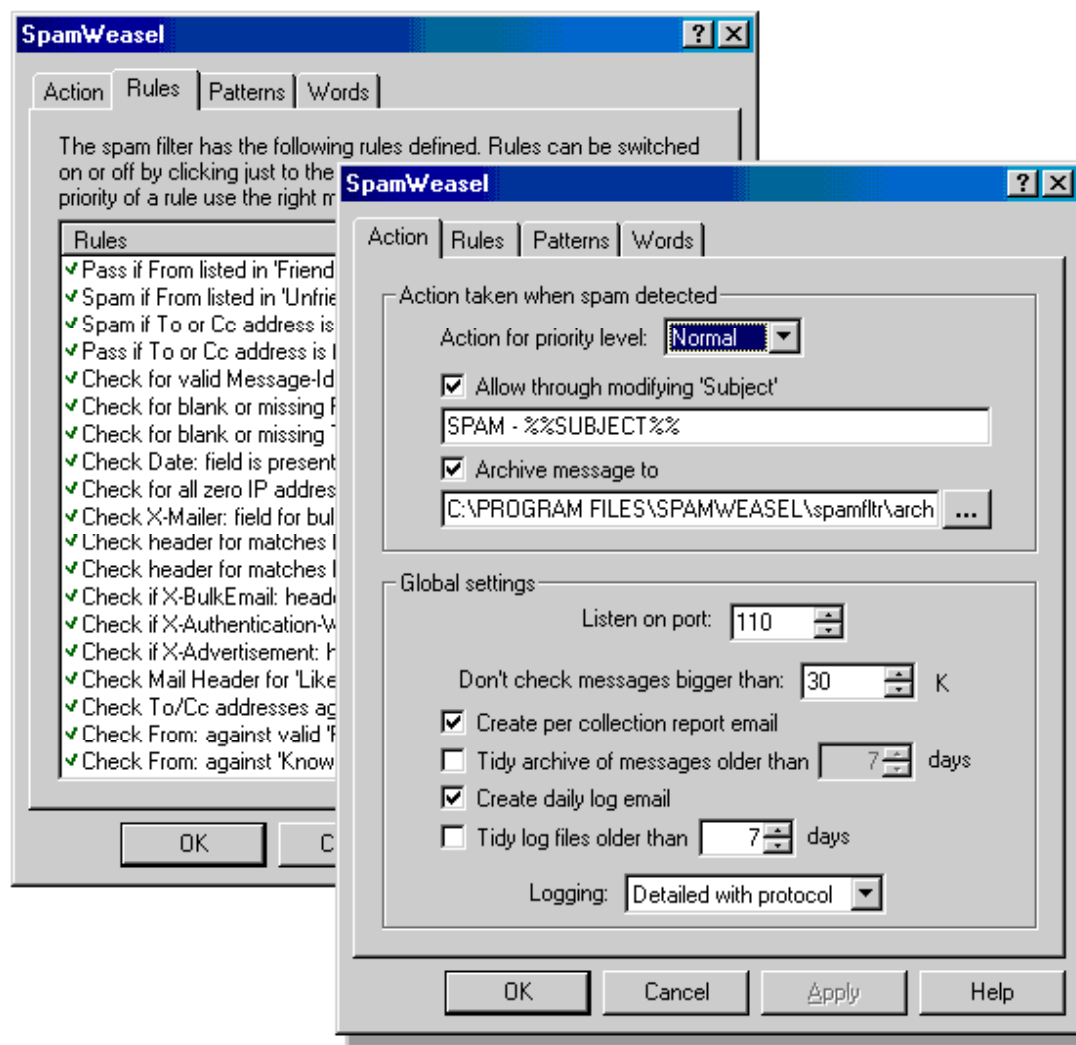
SpamWeasel removes the spam before it gets into the inbox

It either deletes or archives the suspected spam mail which enters user's mailbox by placing a warning message

SpamWeasel supports multiple POP accounts



SpamWeasel: Screenshot



Spytech SpamAgent

Spytech SpamAgent is a powerful email monitoring and filtering tool which gets the emails according to users choice

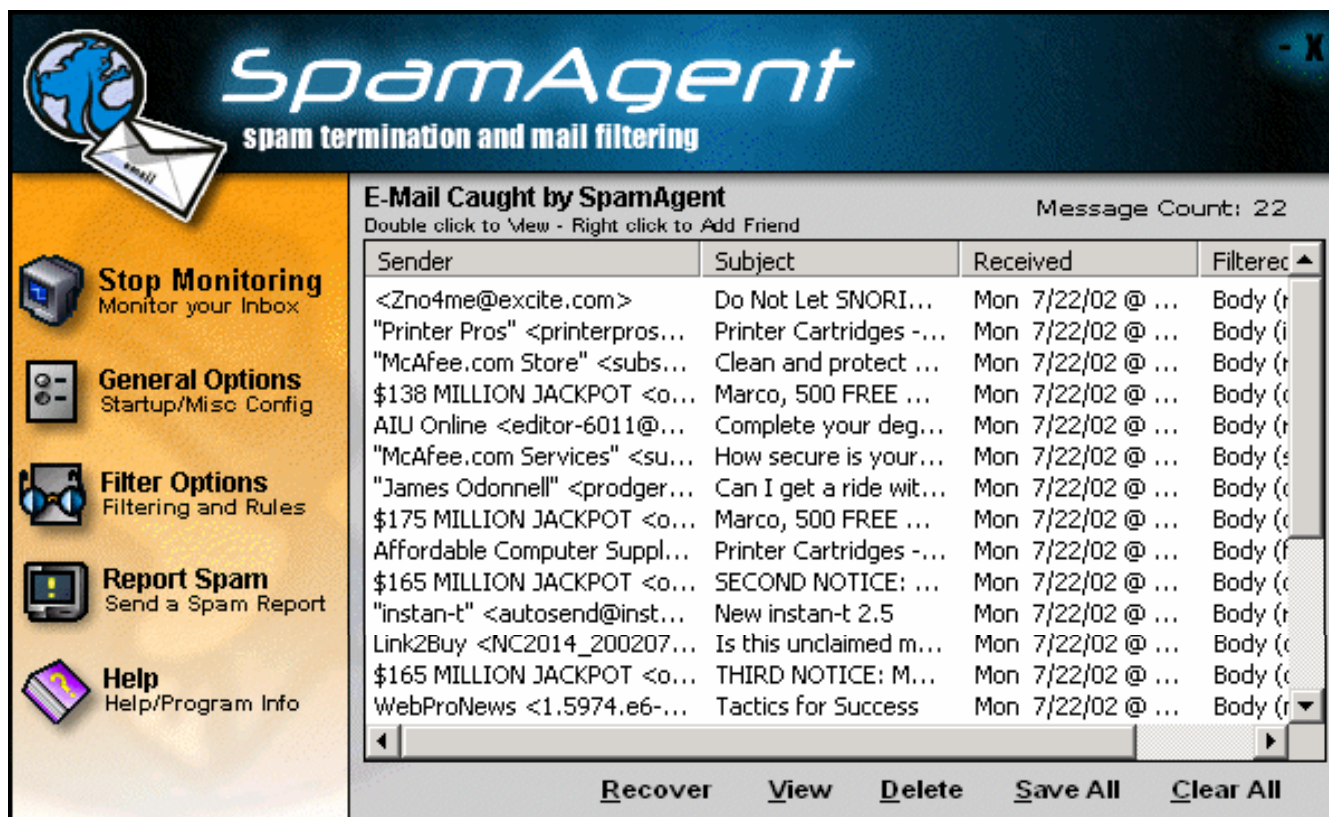
It contains filters which block unwanted and spam mails getting into the inbox

It filters based on the sender, recipient, subject, body, as well as attachment type, forwards, and more

Spytech SpamAgent removes the spam mails from the mailbox but deletes it only after user's acceptance



Spytech SpamAgent: Screenshot



AntispamSniper

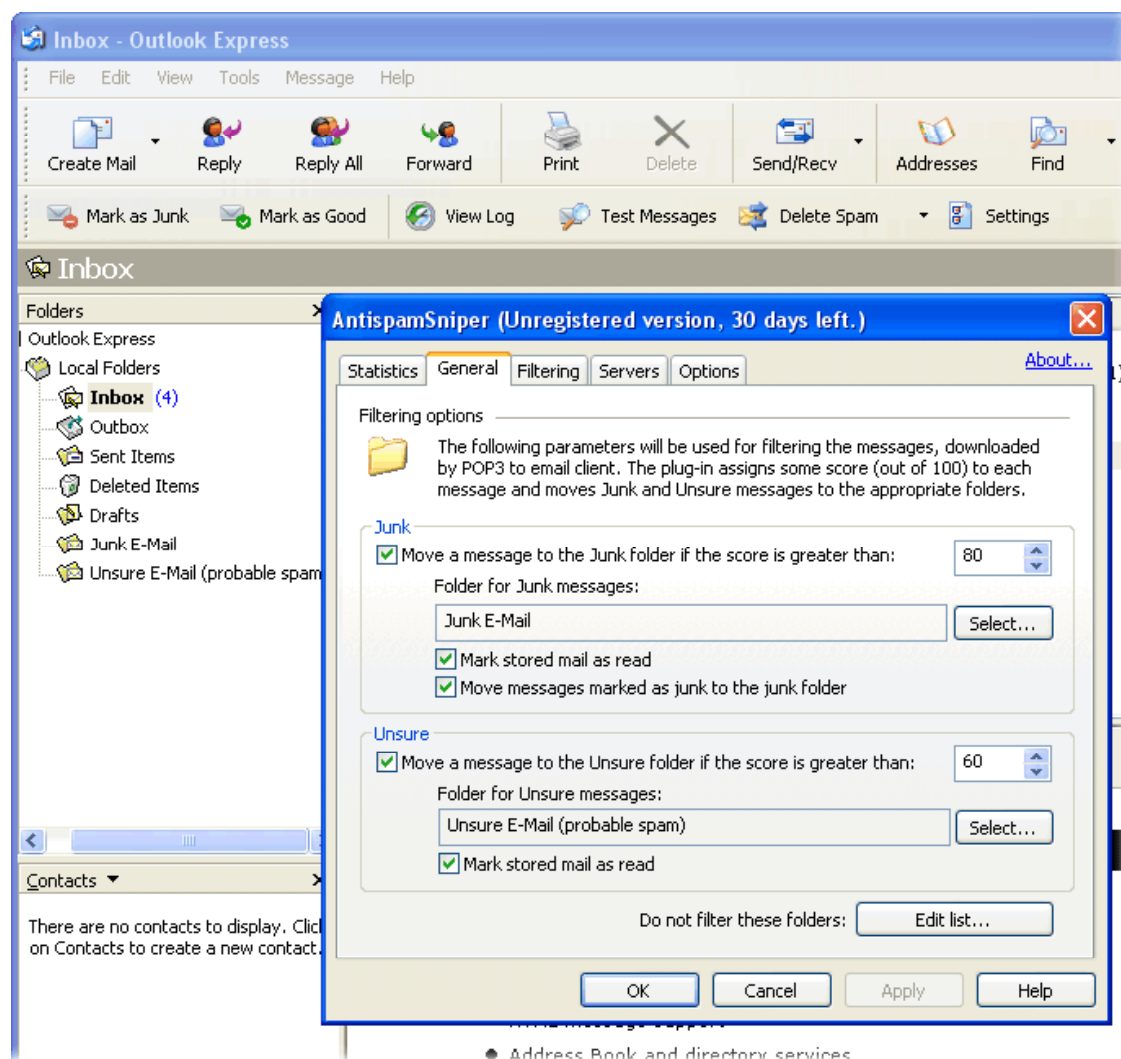
AntispamSniper integrates with Outlook Express to filter incoming mails

It moves the spam mails into junk mail folder which allows user to review and delete it later

Spam filtering techniques include filtering attachments, customizable spam rules, blocking of specific senders, and more



AntispamSniper: Screenshot



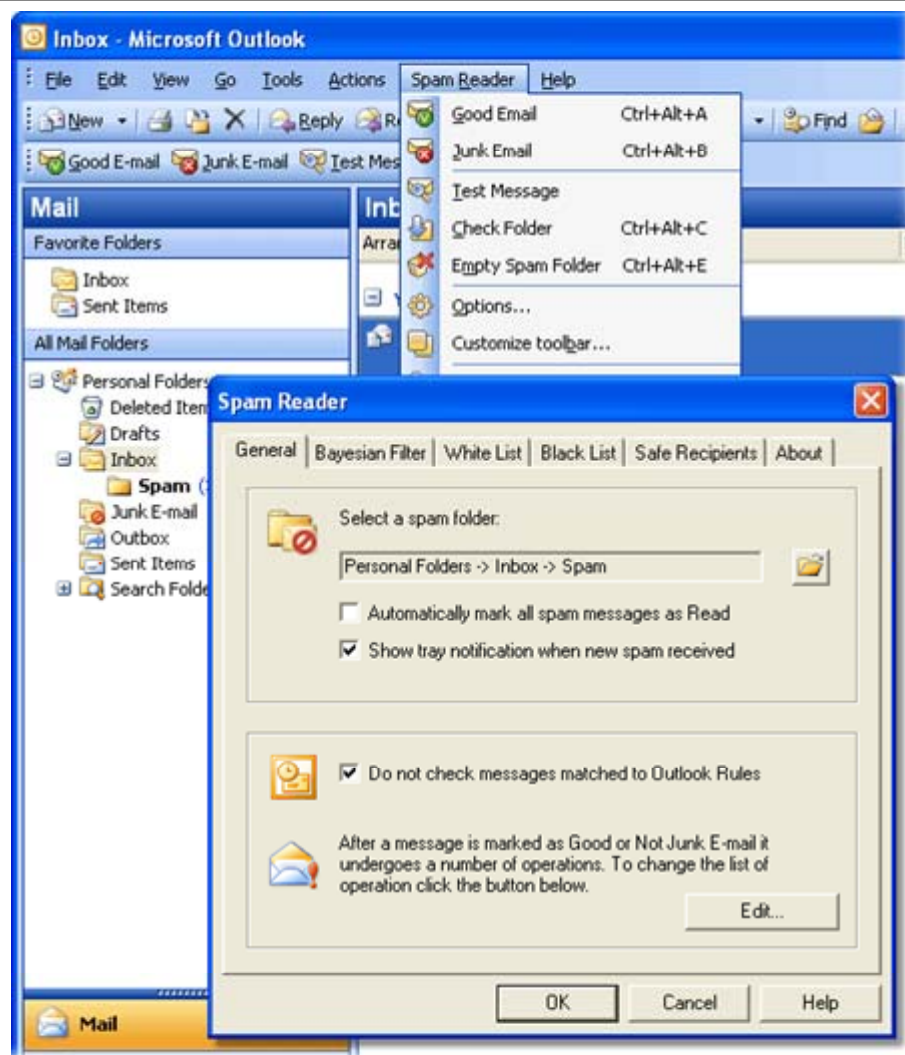
Spam Reader is an anti-spam add-on for Microsoft Outlook

It automatically scans the inbox messages for spam and filters into the spam folder

Spam Reader uses a Bayesian engine which distinguishes between spam or good mails



Spam Reader: Screenshot



Spam Assassin Proxy (SA) Proxy

Spam Assassin Proxy is based on open source software

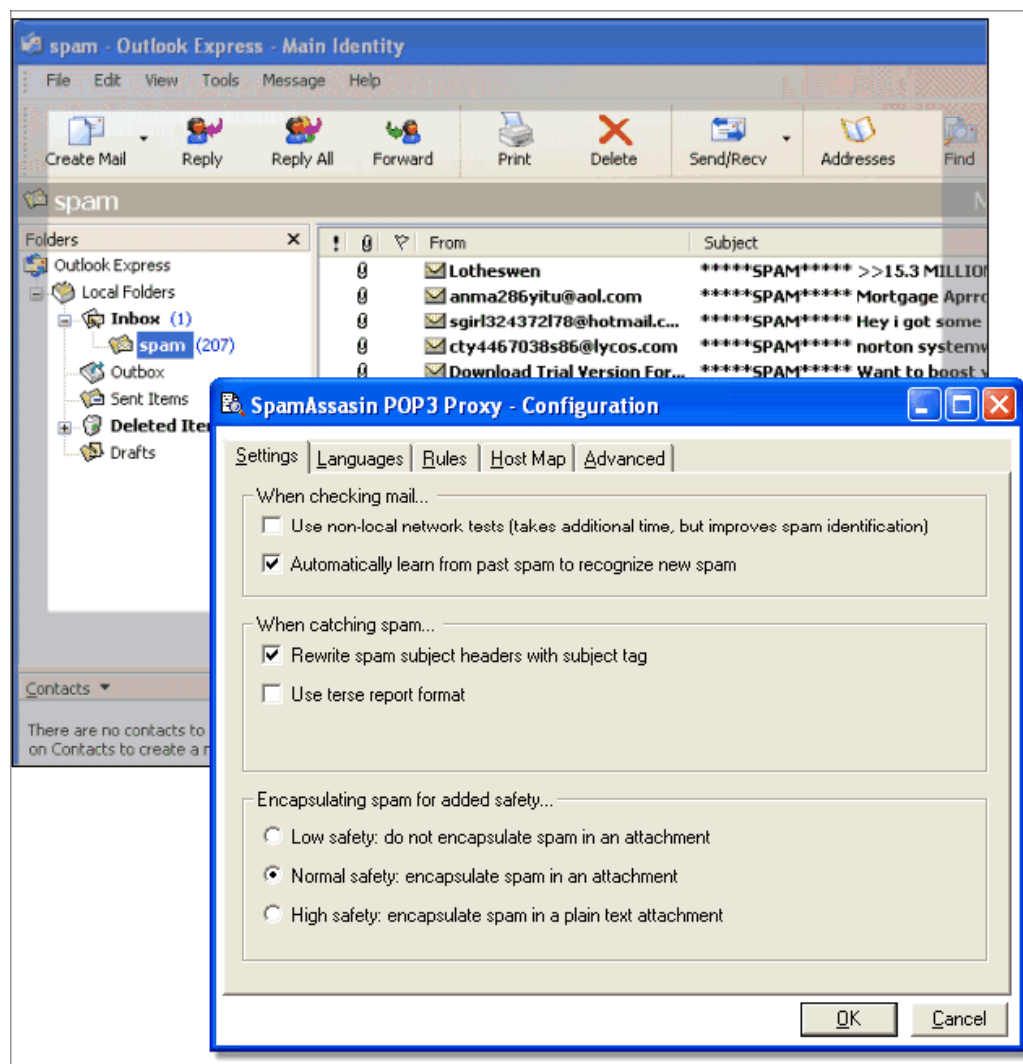
It runs on the local proxy server which is situated between email program and POP3 mail account

Spam Assassin Proxy uses Bayesian filtering which is accurate and detects new spam

It does not delete spam but marks it



SA Proxy: Screenshot



MailWasher Free

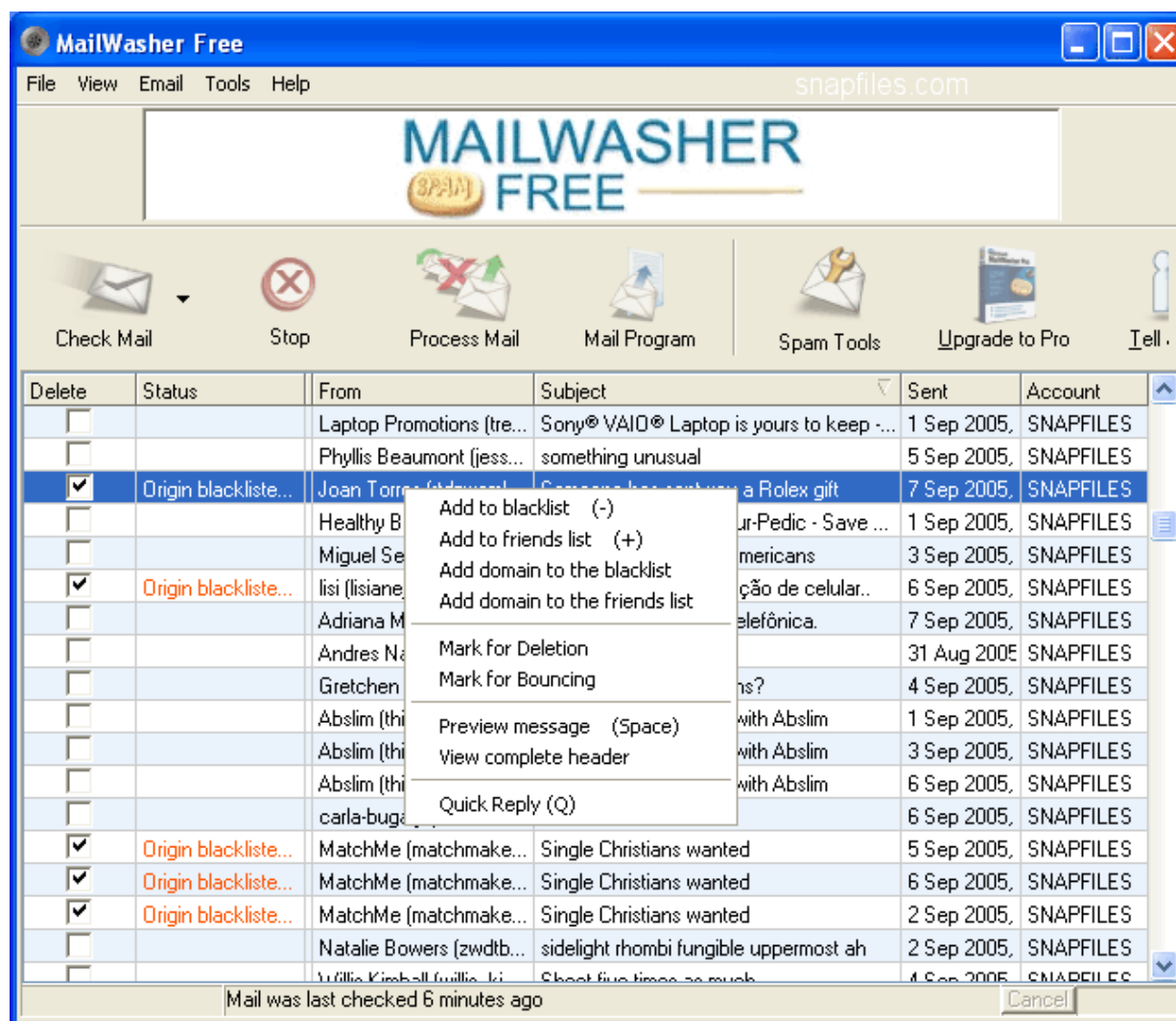
MailWasher Free is used as a spam detection and mail preview tool which allows the user to check mail on server and delete it if spam is found

There are 3 levels of spam detection where the user can specify his/her own filters

It allows to create the user's own spam filter



MailWasher Free: Screenshot



Spam Bully

Spam Bully is an anti-spam tool for MS Outlook

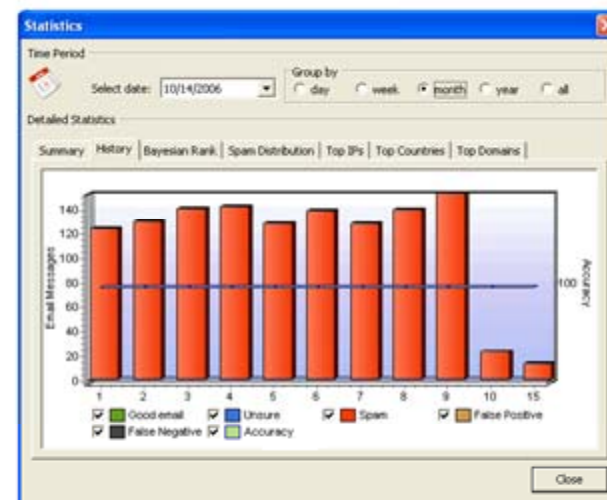
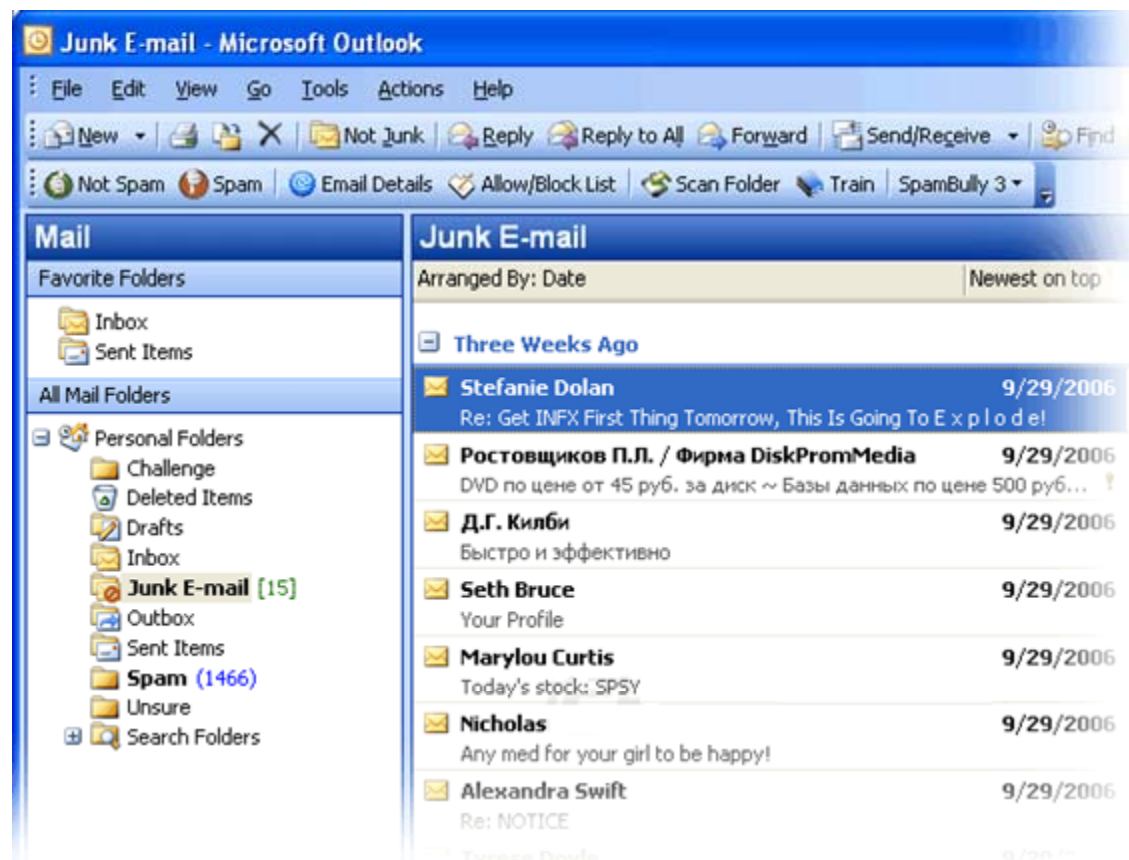
It removes 99 percent of the spam mails from the inbox

Spam Bully moves all spam messages into the spam folder which can be permanently deleted

It can also bounce messages from known spammers, query emails sent from unfamiliar emails, block selected attachments types, and more



Spam Bully: Screenshot



Spamming is all about populating the user's inbox with unsolicited or junk emails

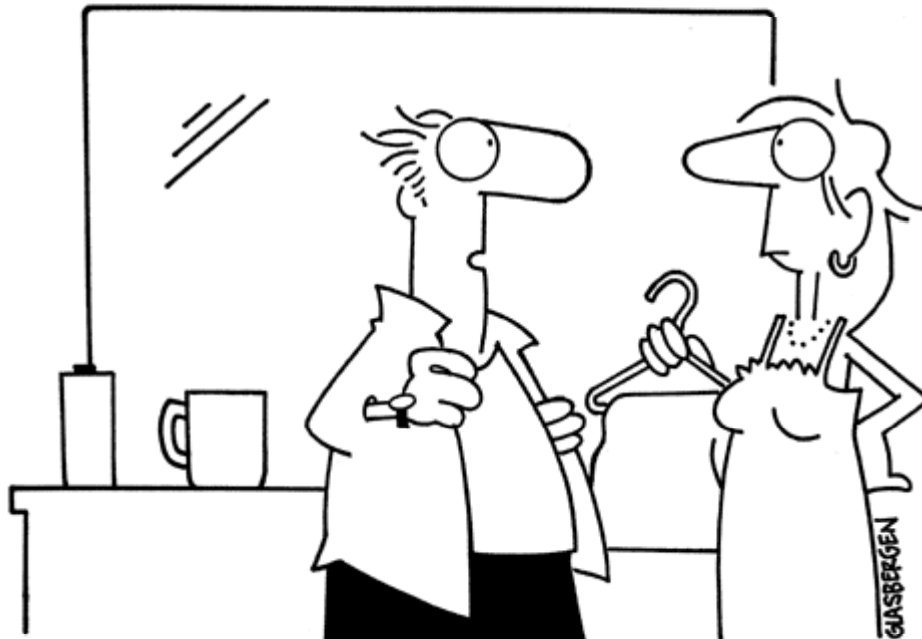
Spammers gets access to the email ID's when the user registers to any email service, forums, or blogs by hacking the information, or registers as genuine users

Spiders are used which searches the code in web pages that looks as email ID's and copy it to the database

The spam message is enclosed as an image in the mail to make the anti spam software trust the source

AEVITA Stop SPAM Email helps to hide email addresses from spambots

Copyright 2003 by Randy Glasbergen. www.glasbergen.com



"I get to the office around 8:45, pour myself a cup of coffee, turn on my computer, delete all the spam, and then it's time to go home."

Copyright 2003 by Randy Glasbergen.
www.glasbergen.com



**"It's not the most sophisticated Spam blocker
I've tried, but it's the only one that works!"**