Spy Emergency 2007

User Manual

Document version 1. 2 EN (18. 10. 2007)

Copyright (c) 2007 NETGATE Technologies s.r.o. All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<u>http://www.openssl.org/</u>)

This product uses compression library zlib Copyright (C) 1995-1998 Jean-loup Gailly and Mark Adler.

All other trademarks are property of their respective owners.

Content

1. Introduction	
1.1. Basic Protection Concepts	3
1.1.1. Prevention	
1.1.2. Automatic Updates	3
1.1.3. Demand Scanner	3
1.1.4. Scheduling	3
1.1.5. Malware Removal	3
1.1.6. The Cage	
1.2. Detection Technologies	4
1.3. Supported Operating Systems	4
2. Installation	
2.1. Installation from website	4
2.2. Installation Process	4
3. Program Activation	8
3.1. Trial Version	
3.2. Purchase	9
3.3. Registration	
4. Working with Spy Emergency 2007	9
4.1. System tray icon	
4.2. Memory Shields	
4.3. Window handling icons	
5. Application Interface	
5.1. Status	
5.2. Scanner	
5.3. Removal	
5.4. The Cage	
5.5. Options	
5.6. Keep List	
5.7. News	
5.8. Buy/About	
5.9. Technical support	
6. Anti-Spam and Anti-Malware Proxy	
7. Analyzer Tool	
8. Signature Updates	
9. Command line interface	
10. Shell extension	
11. Technical support	28

1. Introduction

This user manual introduces overview of all features and technologies provided by **Spy Emergency 2007**.

1.1. Basic Protection Concepts

1.1.1. Prevention

Most threats today come from web sites, emails or as content with other installed software. Users should take care when visiting suspicious site, do not open e-mail attachments about its content are not sure and be careful when installing new software. **Spy Emergency** scans web site URLs that may contain possible threats, scans your e-mail attachments for malware (malicious software), scan and classify your e-mails for spam and scans programs before they are executed for possible threats.

1.1.2. Automatic Updates

Every day new spyware, malware and spam is created that may be possible threat for your computer. It is recommended to allow automatic updates to be turned on to receive regular updates on new threats for your better protection.

1.1.3. Demand Scanner

Demand scanner allows users to manually scan for malware that was installed prior **Spy Emergency** installation or is not activated on your computer.

1.1.4. Scheduling

Scan scheduling is convenient feature that simplifies scanning of your computer. Selected scans are performed based on your personal settings at specified regular time.

1.1.5. Malware Removal

It is important to note that some (but not all) malware or spyware can be removed from your computer.

1.1.6. The Cage

Part of the removal process is the backup of malware in the Cage. It is place where malware is safely stored and encrypted in inactive state so it cannot harm your computer.

1.2. Detection Technologies

Spy Emergency 2007 uses the following technologies to detect malware and spam:

- **Signature scanning** searching for specific signatures that are characteristic to individual malware located at different places including files and registry keys.
- Heuristic analysis identifies malware based on its common behavior.
- Bayesian analysis identifies spam messages based on probability

1.3. Supported Operating Systems

Spy Emergency 2007 is compatible with Windows Vista (64-bit and 32-bit), Windows XP (32-bit) and Windows 2000 (32-bit) operating systems.

2. Installation

Spy Emergency 2007 can be installed either from the installation file available on your installation CD, or can be downloaded from Spy Emergency website: <u>www.spy-</u><u>emergency.com</u> in download section. Latest version is always available on the mentioned website.

2.1. Installation from website

Visit **Spy Emergency** website at <u>www.spy-emergency.com</u>, go to the **Download** section of the website and select appropriate **Download Now** link based on your language preferences. Save the installation file to your disk. Start the installation by executing (double-clicking) the downloaded setup file.

2.2. Installation Process

Please note: It is recommended that you close all other running applications before starting the installation process; including other security applications that might block the installation. You have to start installation process under administrator account.

a) Double-click on the installation setup file to begin the installation process.

b) Select the preferred installation language and click on **OK** button.

Select S	ietup Language	×
	Select the language to use during the installation	c
	English	
	OK Cancel]

Note: This is the language of the installation program. You can change the language of the **Spy Emergency** later on the **Skin/Languages** setup wizard page. To change the language after installation, right-click the system tray icon and select the **Options** menu. Select from **Active Language** menu your preferred language and press the **Apply** button.

c) When setup begins click on *Next* to view the *License Agreement* dialog. Click on *I* accept the agreement to accept Spy Emergency License Agreements terms and conditions.

🕹 Setup - Spy Emergency	= 🗆 🔀
License Agreement Please read the following important information before continuing.	
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.	
Spy Emergency 2007 License Agreement	
Please read the terms and conditions of this license agreement ("License") before installing Spy Emergency ("Software"). By installing and using the Software you accept and agree to the terms of this License. This License constitutes the entire agreement concerning the Software between you and NETGATE Technologies s.r.o., Prievidza, Slovak Republic. If you do not agree with these terms and conditions, immediately uninstall the Software. The term "Software" includes, and these terms and conditions also apply to, any updates, modifications and upgrades	•
 I accept the agreement 	
I do not accept the agreement	
< Back Next >	Cancel

d) Choose the destination folder for the installation, and then click on **Next** button.

💩 Setup - Spy Emergency	= 🗆 🔀
Select Destination Location Where should Spy Emergency be installed?	
Setup will install Spy Emergency into the following folder.	
To continue, click Next. If you would like to select a different folder, click Browse.	
C:\Program Files\NETGATE\Spy Emergency 2007 Browse	
At least 33,8 MB of free disk space is required.	
< Back Next > C	Cancel

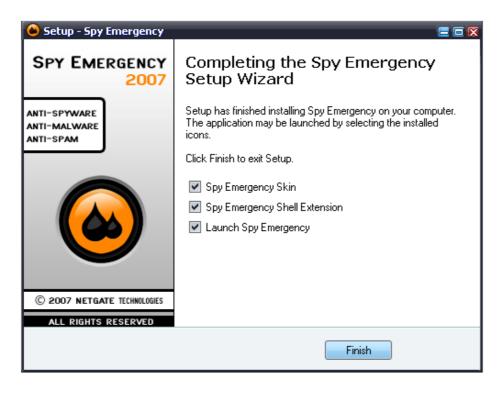
e) Select the *Start Menu* folder where the program's shortcuts will be located. Click on *Next* to continue.

🐵 Setup - Spy Emergency	= 🗆 🔀
Select Start Menu Folder Where should Setup place the program's shortcuts?	
Setup will create the program's shortcuts in the following Start M To continue, click Next. If you would like to select a different folder, click	
Spy Emergency 2007	Browse
< Back Next >	Cancel

f) Check the additional tasks that should be performed. It is recommended to check all options. Click on *Next* to continue.

🙆 Setup - Spy Emergency	
Select Additional Tasks Which additional tasks should be performed?	
Select the additional tasks you would like Setup to perform while installing Spy Emergency, then click Next.	
Additional icons:	
💌 Create a desktop icon	
💌 Create a Quick Launch icon	
< Back Next > Ca	incel

g, To complete the installation process click on *Finish*. You can check individual options that will be performed during finalization process. It is recommended to check all options.



h, If you have selected skin selection in the previous step, Spy Emergency Language and Skin wizard will be shown. Select preferred skin and language that matches your individual taste.

5py Emergency - Ski Skin/Languages:	n/Languages:	(
ctive skin:		
 Default 	Blue	C Green
Red	Silver	○ White
ctive language: English	h 💌	
		ОК

After the installation process is finished, **Spy Emergency 2007** will launch automatically.

3. Program Activation

3.1. Trial Version

From the spy emergency website you can download the trial version of **Spy Emergency 2007**. After the installation, this trial version will run for 15 days. This version is fully functional but only one signature database updates is performed at program installation.

Within 15 days you have to register the program using registration information number to activate the full version of **Spy Emergency 2007**. The purchased registration information can be entered at any time of this trial period or after this period.

3.2. Purchase

In the **Buy** menu select the **Buy Now** button. Default Internet browser will be launched with the registration page.

3.3. Registration

In the **Buy** menu select the **Enter serial** button. Registration dialog will show up. With purchase of **Spy Emergency 2007** you have received registration information; **registration name, registration e-mail** and **serial number**. This information has to be exactly entered into registration dialog. Please note that serial number only contains characters **A-F** and **numbers**.

	Spy Emorgoney 2007	 ? i
	Spy Emergency 2007 Anti-Spyware * Anti-Malware * Anti-Spam	
Status - p	Please enter registration information:	
Scan - L	The Product is licensed to:	
Remove - L	1	
The Cage - R	Order email:	
Options - /	Serial number:	
Keep List		
News	OK Cancel	
Buy	Enter serial Buy Now	
Support		

4. Working with Spy Emergency 2007

After you have successfully installed **Spy Emergency 2007** on your computer, the **Spy Emergency 2007** icon will appear on your desktop. Double-clicking the icon will launch the **Spy Emergency 2007**. This interface allows you to configure individual aspects of the application.

4.1. System tray icon

Once the application is started, you can see a small orange/black icon in the system tray, indicating that the application is running. By right-clicking on the tray icon, a context menu will popup:

۵	Spy Emergency
۹	Start Scan
≫	Options
۲	News
~	Enable Home Page Shields
>	Enable Memory Shields
>	Enable Tracking Cookies Shields
~	Load at Startup
0	About
×	Close
	🙀 Registry Editor 📃 📃 🥹

The following options are available:

- Spy Emergency click this option to hide or show the main application screen.
- *Start Scan* this option will automatically start scanning of your system.
- **Options** this option will open application configuration dialog.
- **News** this option will open news dialog.
- **Enable Home Page Shields** by checking this option, Spy Emergency will protect your web browser homepage and notify you about its change.
- **Enable Memory Shields** by checking this option, Spy Emergency check every program for malware before it is executed.
- **Enable Tracking Cookies Shields** by checking this option, Spy Emergency will check created cookies for tracking cookies and remove it in real-time (Internet Explorer only).

Load at Startup – by checking this option, Spy Emergency will be launched every time your Windows operating system is started.

About - this option will show application about dialog.

Close - this option will quit the application.

4.2. Memory Shields

Spy Emergency 2007 resident memory shields protect your computer against malware that tries to run on your computer. It checks every program that is starting up for malware. It is recommended to have **memory shields** turned on. The **status** of the memory shields can be easily seen by pointing on program icon in the system tray.

When a suspicious process is **detected**, the memory shields will notify you about the possible threat and offer you options on how to proceed with the detected file.

Spy Emergency 2007 Anti-Spyware * Anti-Malware * Anti-Spam
Warning: Detected infection!
Infection name:
Trojan Simulator
File location:
e:\trojansimulator.exe
Infection type: Misc
Description:
Generic category for software that does not match other categories and may be potentially unwanted f
Remove To Keep List Run scan Close

This dialog offers the following actions:

Remove – removes detected file from the system.

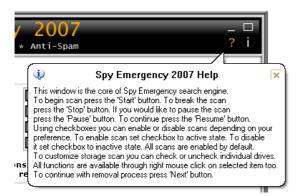
To Keep List – adds this threat to the Keep List. Software on the Keep List will next time ignored and the user will be not notified about its presence.

Run scan – system scan will be initiated to find all possible threat in the user system.

Cloase – dialog will be closed without any action.

4.3. Window handling icons

There are four icons at the right-top corner of the program interface. **Minimize** button (topleft) allows you to minimize application windows to the system tray. **Maximize/Restore** (top-right) button allow you to maximize application window to the maximum width and height of your desktop and restore it to the previous size. **Help** (bottom-left) button displays help information about currently open dialog. **Information** (bottom-right) button will show about dialog.



5. Application Interface

5.1. Status

The **status** dialog allows fast access to the common program function and shows statistics information about individual components.

~))	Status				
	System Status:				
Status	Last performed scan:	20	07/06/03	Scan Now	
	Active scan type:		Standard	Deep	
Scan	Total malware detected:	82	7	Reset	View log
emove	Files in the cage:	15	7	Show	
ie Cage	Protection Status:				
	Web protection:	On	Memory	protection:	On
ptions	Objects scanned:	609	Objects	scanned:	164
ep List	Objects infected:	0	Objects	infected:	1
News	Automatic updates:	On	Anti-Spa	m protection:	On
	Last update:	2007/06	03 Message	s scanned:	45
About		Iledate No.		s infected:	0
upport		Update Now	Spam m	essages:	9

Last performed scan – shows the date when last system scan was performed.

Active scan type – allows switching between **Standard** and **Deep** scan types. **Standard scan** is faster than Deep scan; it checks only common file extension for malware and use level 1 heuristics analysis. **Deep scan** is more precise scan; it checks files based on its content than on file extension and use level 2 heuristics analysis. Level 2 heuristics take longer by may bring in some cases better results. Standard scan is the default settings and is sufficient for malware detection in most cases.

Total malware detected – shows total count of malware detected; this count can be reset by pressing the **Reset** button.

Files in the cage – shows total count of malware in the cage; to show the content of the cage press the button **Show**.

Scan Now – this button starts system scanning.

View logs – shows log files generated by Spy Emergency.

Object scanned – shows the count of checked items

Object infected – shows the count of infected items

Web protection – shows the status of the web shield and anti-phishing shield.

Memory protection – shows the status of the memory shield.

Anti-Spam protection – shows the status of the anti-spam protection.

Messages scanned – shows the count of checked messages for malware and spam.

Messages infected – shows the count of the messages that contains malware.

Spam messages – shows the count of the messages that were classified as spam.

Automatic updates – shows the status of the automatic updates. It is recommended to have this option turned on.

Last update – shows the date when the check for update was lastly performed.

5.2. Scanner

The **scanner** dialog is the place where the **scanning engine** can be controlled in a convenient way. This dialog can be accessed by pressing **Scan** in the left menu.

	Spy Emer Anti-Spyware * A	nti-Malware	* Anti-Spam ?
	Scan		
	Scan memory on your	system	A:\ Floppy (A:)
Status	Scan registry on your Scan cookies on your		✓ C:\ C (C:) D:\ D (D:)
Scan	🖌 Scan drives on your s	ystem	E:\ E(E:)
Remove	This list contains dete	ected infectio	ns: (hit the 'Next' button to continue with the removal)
The Cage	Signatures in database:	140145	+ 🐇 No infections in the list.
Options	Processes scanned:	0	+ 🛧 Press the 'Start' button
	Registry items scanned:	0	🕈 🛓 To start new scan
Keep List	Cookies scanned:	0	
News	Files scanned:	0	
	Infections found:	0/0	
About	Elapsed time:	00:00	Start Pause Next
Support	Current location:	Not active.	

Scan memory on your system – if this item is checked; program will scan **memory** for malware.

Scan registry on your system – if this item is checked; program will scan **registry** for malware.

Scan cookies on your system – if this item is checked; program will scan **cookies** for tracking cookies.

Scan drives on your system – if this item is checked; program will scan **files** for malware. To check only specific system drives; use checkboxes near drive names in the top-right side of this dialog. Custom location can be added by clicking on **Add custom path...** item.

Signatures in database – shows the total count of detection signatures in the database.

Processes scanned – shows the count of scanned process in memory.

Registry items scanned – shows the count of scanned registry keys.

Cookies scanned – shows the count of scanned cookies.

Files scanned – shows the count of scanned files.

Infections found – shows the total count of detected infections. The first number is the total count of different families detected during scan; the second number, separated by slash, is the total number of traces detected during scan.

Elapsed time – shows the time since the start of the system scan.

Start – pressing this button will start the system scan.

Pause – pressing this button will cause the system scan to pause.

Next – pressing this button will guide user to the removal wizard dialog. This button is enabled when there are detected infections only.

Malware detected during scan is listed above the Start/Pause/Next buttons in the detected infections list.

Current location – this field shows actual file or registry being checked or action being performed.

5.3. Removal

The **removal** dialog allows removal of all detected infections. This dialog can be accessed by pressing **Remove** in the left menu. This dialog is available only after some infections have been detected.

	Remove			
	Select infections to re	emove: (softwa	re will be hold in the ca	ige for later restore
Status	+ 🗹 🗶 Ace Club Casino	M	edium 🔲 Action: Re	move
Scan				
Remove				
he Cage				
Options				
eep List				
News				
About	Select all	Deselect all	1	
	Seleccan	beserect an		

Select all – selects all items in the list.

Deselect all - deselects all items in the list.

Details – show information about detected item.

To Keep List – selected items will be added to the keep list; this infection will be ignored in the next scan.

Remove – removes selected infections.

Action – default action recommended by the program. Only experienced user should modify these settings. **Ignore** – item will be ignored and not removed. **Remove** – item will be removed.

Note: Under Windows Vista confirmation dialog will popup. You have to allow this action to successfully remove selected items.

5.4. The Cage

The **Cage** is the place where all removed infections are kept.

	The Cage		
\smile		ed infections: (Use 'Delete Forever' to store' to bring infections back to life	
Status	ке	store to bring intections back to life,)
and the second	+ 🔲 🐁 Acropolis	Low	
Scan	🕈 🔲 🐇 Trojan.Emcodec.B	High	
Remove	+ 🔲 🐁 VirusBurst	Low	
Remove	+ 🔲 🐁 DriveCleaner	Low	
The Cage	+ 🔲 🐁 Trusted sites	Low	
	+ 🔲 🐁 SystemDoctor	Low	
Options	+ 🔲 🐁 Worm.Stration	High	
	+ 🔲 🐁 Worm.Mydoom	High	
Keep List	+ 🔲 🐁 7adPower	High	
News	+ 🔲 🐁 Trojan.EICAR	High	
	🕈 🔲 🐁 Trojan.Emcodec.E	High	
About	🕈 🔲 🗶 Trojan Simulator	Low	

Select all – selects all items in the list.

Deselect all – deselects all items in the list.

Delete forever – infections will be totally removed from the system and cannot be restored again.

Restore – restores items to the previous place.

Note: Under Windows Vista confirmation dialog will popup. You have to allow this action to successfully restore/delete forever selected items.

5.5. Options

The **Options** dialog allows configuration of individual functions of **Spy Emergency 2007**.

Spy Emergency Tab:

	Spy Emergency Active shields Database Miscellaneous Engine Anti-Spam Scheduling:
Status Scan Remove	Scheduling: Type of scan: Enable Sunday Thursday on: Monday Friday Scan at: Tuesday Friday 8:00 Wednesday Saturday
he Cage Options	Startup:
eep List	Run at Windows startup
News	Skin/Languages:
About	Active skin: Default + Active language: English + Apply

Scheduling – scheduling allows users to run specified system scan periodically. To enable scheduling check the **Enable** button, select hour, check the day and type of the scan.

LSP Fixing – repairs damaged LSP stack by malware at program startup. Note: you have to run Spy Emergency as administrator under Windows Vista to perform this action.

Run at Windows startup – Spy Emergency will be launched at system startup.

Active skin – skins change the look of buttons and menus of the program; active skin is the currently selected skin.

Active language – is the currently selected language. To apply changed skin and language settings press the **Apply** button.

Active shields Tab:

	Anti-Spyware * Anti-Ma			
	Spy Emergency Active shi	elds Database	Miscellaneous	
\smile	Engine	Anti-Spam		
Status	Active shields:			
	Memory shield:	Active	Inactive	
Scan	Cookie shield:	Active	Inactive	
	Alternate Data Stream shield:	🗹 Active	Inactive	
Remove	IE Search Page shield:	🗹 Active	Inactive	
	ActiveX shield:	Active	Inactive	
The Cage	Web and Anti-Phishing shield:	Active	Inactive	
Options	Spyware Communication shield	: 🗹 Active	Inactive	
options	Browser Helper Object shield:	🗹 Active	Inactive	
Keep List	Startup Programs shield:	🗹 Active	Inactive	
	Trusted Sites shield:	Active	Inactive	
News	Windows Logon shield:	🗹 Active	Inactive	
	Home page shield:	🗹 Active	Inactive	
Buy	🧔 🗹 Internet Explorer	http://www.google.sk/	Update	
Support	🧶 🗹 Mozilla Firefox	http://www.google.sk	Update	
auphon	n Opera Browser	http://www.google.com	Update	

Memory shield – scans every starting process for possible threat. When threat is detected user notified and can select appropriate action. If **automatically remove with backup** option is selected; item is removed to the cage without user confirmation.

Cookie shield – removes tracking cookies in real-time. Note: Internet Explorer cookies only.

Alternate Data Stream shield – blocks processes starting from ADS streams. Note: Memory shield have to be enabled.

IE Search Page shield – protects web browser search page settings. Note: Internet Explorer only.

Active-X shield – blocks malware active-X elements. Note: Internet Explorer only.

Web and Anti-Phishing shield – blocks access to malware Internet locations.

Spyware Communication shield – blocks malware communication to the Internet.

Browser Helper Object shield – blocks malware BHO elements. Note: Internet Explorer only.

Startup Programs shield – blocks malware from setting up itself at system startup launch.

Trusted sites shield – blocks malware from adding trusted sites items. Note: Internet Explorer only.

Windows logon shield – blocks malware from setting up itself to be launched together with winlogon process at system startup launch.

Home page shield – notifies user about home page modification and allows changing the homepage to the previous settings. Note: Internet Explorer, Mozilla Firefox, Opera only. To modify home page of the browser, users should modify input boxes near to the browser names and press the **Update** button.

Database Tab:

Spy Emerg	Jency 2007 – C i-Malware * Anti-Spam ? i
	e shields Database Miscellaneous ngine Anti-Spam
Status Automatic updates:	
Scan Database	Update Now
Remove News	Update interval: 60 min 🔹
The Cage Proxy:	
Options	Login:
Keep List Port:	Password:
News Proxy Type: HTTP	• Update
About	
Support	

Automatic updates – this function allows user to automatically update signature databases. When allowed by checking **Database**, **Anti-Spam** database and/or **News**; Spy Emergency will check for new signatures at program startup and at regular interval specified by the **update interval** value. To update manually press the **Update Now** button.

Proxy - if the user use a proxy server to connect to the Internet, then it will be necessary to specify the proxy server settings so that **Spy Emergency 2007** can access the Internet for updates.

Note: If you do not use a proxy server connection then do not modify these settings.

Host - enter the hostname for the connection.

Port - enter the port number for the connection.

Proxy *Type* - select the type of connection *HTTP*/*Socks5* for the proxy server.

Login - enter the login name for the proxy connection.

Password - enter the password for the proxy connection.

To **apply** the proxy settings press the **Update** button.

Miscellaneous Tab:

Spy Emerg	ency Act	tive shields Database Miscellaneous
Status	ge Settings:	Engine Anti-Spam
Status Search Page	e:	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=iesearch
Scan Default_Pag	je_URL:	http://www.microsoft.com/isapi/redir.dll?prd=ie&pver=6&ar=m
Remove Default_Sea	arch_URL:	http://www.microsoft.com/isapi/redir.dll?prd=ie&ar=iesearch
Local Page:		c:\windows\system32\blank.htm
he Cage SearchAssis	stant:	http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchasst.h
Options	earch:	http://ie.search.msn.com/{SUB_RFC1766}/srchasst/srchcust.h
Ceep List		
Clean Tem	porary files d	
About Run Analy	Run Analyzer Tool to report unknown malware:	
Support		

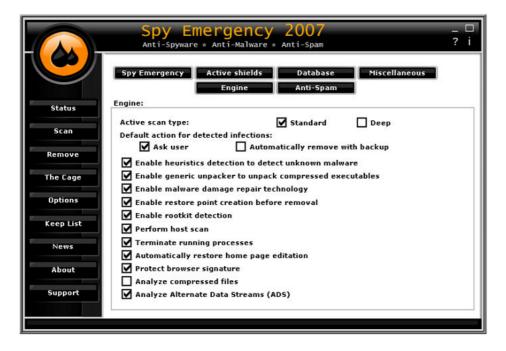
IE Search page settings - these Internet Explorer values are protected when **IE Search Page shield** is active. Edit individual values to your preference. Only experienced users should modify these settings.

Clear Temporary files directory – to remove all files from the local user temporary directory press the **Clean** button. This directory contains temporary files created by applications.

Clear Temporary IE directory – to remove all files from the local user Internet Explorer browser cache press the **Clean** button. This directory contains web pages cache and files saved by the Internet Explorer.

Run Analyzer Tool to report unknown malware – Analyzer Tool is a simple tool to report log files from your system. These files help to isolate undetected malware problems at Spy Emergency research center. To run this utility, press the **Run** button.

Engine Tab:



Active scan type – allows switching between Standard and Deep scan types.

Default action for detected infections – default action performed when infection is detected: **Ask user** – user is notified and have the option to choose appropriate action; **Automatically remove with backup** – infection is moved to the cage without user confirmation.

Enable heuristics detection to detect unknown malware – heuristics detection allows to detect unknown malware not in the program database but using common malware behavior inspection.

Enable generic unpacker to unpack compressed executables – many executables are compressed by authors to make it harder for antivirus software to detect them; generic unpacker tries to uncompress them.

Enable malware damage repair technology – some malware makes user system unusable when it is removed from a system. This feature tries to repair damages produced by such malware.

Enable restore point creation before removal – when enabled program will create restore point before removal; restore points can be used to revert system to the previous state.

Enable rootkit detection – rootkits are processes that try to hide itself from the user and detection techniques.

Perform host scan – scans and removes ip addresses added by malware from the system host file.

Terminate running processes – terminates malware processes before its removal; this ensures better removal function.

Automatically restore home page editation – some malware blocks home page editation; this function enables editation again. Note: Internet Explorer only.

Protect browser signature – modifies your browsers name signature so the remote server does not know your real browser name. This makes it harder to perform specifics attacks to your system. Note: some browsers and sites may not work properly with this options turned on.

Analyze compressed files – when enabled Spy Emergency will scan inside compressed archives like zip, rar ...

Analyze Alternate Data Streams (ADS) – when enabled Spy Emergency will scan ADS streams on NTFS volumes.

Anti-Spam Tab:

	Spy Emergency 2007 Anti-Spyware * Anti-Malware * Anti-Spam	o i
	Spy Emergency Active shields Database Miscellaneous Engine Anti-Spam	
Status	Anti-Spam:	-
Scan	 Enable anti-spam and malware e-mail protection Add signature to every checked e-mail 	
Remove	Filtering proxy server ports (POP3, IMAP, POP3 SSL, IMAP SSL): 8211 8212 8213 8214	
The Cage	Disable automatic redirection for the following processes:	
Options		
Keep List	Friends/Enemies list:	
News	Delete	
About		
Support	▼	
		_

Enable anti-spam and malware e-mail protection – this feature checks every incoming e-mail for malware and spam.

Add signature to every checked e-mail – when enabled Spy Emergency will add header to the end of each e-mail notifying user that the mail was checked.

Filtering proxy server ports (POP3, IMAP, POP3 SSL, IMAP SSL) – filtering proxy server is a proxy server that listen at specific ports and inspects every e-mail for malware and spam. To change filtering proxy ports change individual input fields. Only experienced users should modify these settings. Note: system need to be restarted to apply these changes.

Disable automatic redirection for the following processes – by default all POP3 and IMAP traffic is redirected to filtering proxy. To exclude some processes from this redirection enter process name into input field. Only experienced users should modify these settings.

Friends/Enemies list – this list contains e-mail addresses that should be specially handled. E-Mails added as **Friend** are never marked as spam; e-mails added as **Enemy** are always marked as spam. To add new e-mail use **Add...** button, to delete e-mail from the list use the **Delete** button.

5.6. Keep List

The **Keep List** is the list of all software/infections that should be ignored by the system scan. Items on this list will be ignored by all type of scans and memory shields.

	Anti-Spywar	mergency 2007 e * Anti-Malware * Anti-Spam	?
	Keep List		
\smile	Keep list hold	Is all software you would like to exclude from the system scan:	
Status	BearShare P2P	Low	-
Scan	E-Mule P2P	Low	
ocum	GnucDNA P2P	Low	
Remove	Gnucleus P2P	Low	
	Ares P2P	Low	
The Cage	Grokster P2P	Low	
Options	KaZaA P2P	Low	
options	Kazaa-Pad P2P	Low	
Keep List	Kazoom P2P	Low	
	Morpheus P2P	Low	
News	Overnet P2P	Low	
	Red Swoosh P2P	Low	
About	IMesh P2P	Low	
Support	Select all	Deselect all Remove	
	Select all	Deselect all Relifove	-

Select all – selects all items in the list.

Deselect all – deselects all items in the list.

Remove – removes item from the list.

5.7. News

The **News** dialog shows latest information about signature database additions/updates. News is downloaded together with signature database updates.

	Spy Emergency 2007 Anti-Spyware * Anti-Malware * Anti-Spam	?
	News	
\smile	Spy Emergency:	
Status	Current Version: 2006 - build 3.0.325	
	Spyware Database:	
Scan	Version: 331	
Remove	Release: 2007/06/01	
	Important Threats New/Updated:	
The Cage	- Worm.Fanbot	
Options	- Trojan.Spy.Botinok	
	- Rootkit.¥anti	
Keep List	- Backdoor.Virkel	
News	- Trojan.Spy.HTML.Bayfraud	
About	- Worm.RavMon	
About	Totally 936 additions/updates	
Support		

5.8. Buy/About

In the trial version this dialog shows Spy Emergency features; in the registered version this dialog shows information about registered user and database information. After registration the **Buy** button will change to **About** button after next program start.

	Spy Emergency 2007 Anti-Spyware * Anti-Malware * Anti-Spam	_ 🗆 ? i
	How to Buy Spy Emergency What will purchase of Spy Emergency brings you?	
Status	- Protection against latest spyware, adware and internet infections	
Scan	- Life-time update of infection database	
Remove	- Intuitive and clear user interface for spyware removal	
Kelliove	- Latest spyware information	
The Cage	- Resident shield protection	
Options	- Life-time technical support - And much more	
Keep List		
News		
Buy	Enter serial Buy Now	
Support		

Enter serial – by pressing this button user has the option to enter registration information; the registration dialog will popup.

Buy Now – by pressing this button your default browser windows will be shown and the online shop web page will be displayed allowing purchasing the product.

5.9. Technical support

The **Technical support** dialog allows users to send e-mail message to the Spy Emergency technical support team. To send a message fill in email, name and description and press the **Submit** button to send the message. User can additionally add attachment by pressing the ... button.

	Support			
Status	New Spyware Reporting: If you h suspicious application please ru us the output log file.		Analyzer Tool	
	The Spy Emergency Technical Su	upport service is here to h	elp in problematic	
Scan	situations. Please contact our te			
Remove	Your email:*			
(enitove	Your name:*	[
he Cage	Problem description:*			
Options	Problem description.			
eep List	Attachment:			
News	All fields marked with * are required the Internet before submitting. I			
About	patient while uploading.		Submit	
	Log File		Sabilite	

Analyzer Tool – this button will run the Analyzer Tool utility.

Log File – this button will show windows with all generated log files.

6. Anti-Spam and Anti-Malware Proxy

Anti-Spam feature of the **Spy Emergency 2007** allows users to identify unwanted spam messages. Note that not all spam e-mail messages can be detected and some e-mail messages could be incorrectly marked as spam.

Anti-Spam and anti-malware filtering engine is independent of any e-mail client and should work with any POP3 and IMAP servers with or without SSL support. Every message detected

as spam is marked in the subject of the checked e-mail with [SPAM] keyword.

There is extra support for Outlook Express and Windows Mail that allows automatic moving such marked messages to **Inbox-spam** folder. Users of other clients should create message rules for such functionality. **Note:** System need to be **restarted** after Spy Emergency installation to enable spam moving feature under Windows Vista.

Available Anti-Spam settings are described in the Option section of this manual.

Spy Emergency 2007 use Bayesian method for detecting new spam and signature scanning methods.

Together with anti-spam feature **anti-malware** filtering of incoming e-mails is enabled too. E-mails containing malware in an attachment or suspicious attachment are marked with **warning** and infected files are renamed.

By default programs connecting to common e-mails ports are redirected to the proxy. The proxy can be accessed as any other server manually using the following configuration:

POP3	proxy server: 127.0.0.1 , port 8211
	login: login[server:110] password: password
IMAP	proxy server: 127.0.0.1 , port 8212
	login: login[server: 143] password: password
POP3 SSL	proxy server: 127.0.0.1 , port 8213
	login: login[server: 995] password: password
IMAP SSL	proxy server: 127.0.0.1 , port 8214
	login: login[server: 993] password: password

7. Analyzer Tool

Analyzer Tool is a simple tool to report log files from your system. These files help to isolate undetected malware problems at **Spy Emergency research center**. After execution this utility will start automatically the logging process. When the process is finished the **send dialog** will show up. To send the log file uses should fill in the e-mail address and problem description fields and press the **Send** button.

Spy Emergency Analyz	er Tool SA	E 🗆 🗙 About
and new spyware, adware, Spy Emergency Research (send you a report of isolated p	Analyzer Tool SA. If you have problem with unknown rojan, worm or virus, please send generated logfile to enter. Our research team will contact you shortly and roblems so you can fix them. Please download and run y-emergency com first before submission to remove all Design (1997)	s: seearch@spy-emergency.com y Emergency Homepage www.cod Sey Engergency
	Contact The Spy Emergency Research Center	×
Check Check Sused Modules Used Modules	Spy Emergency Analyzer will now send a generated log file tr Emergency Research Center. The Research Team will analyze you a report of new, potentially unwanted software on Yo Your e-mail: Problem description: Send	it and send D07/D09
Used Modules	C:\Program Files\Spyware Doctor\tools\swpg.DAT	81b5e1a

8. Signature Updates

New malware threats and spam is continually being created and spread very quickly. It is recommended that Spy Emergency 2007 is updated on a regular basis to protect you against all new threats.

	Spy Emergency 2007 Anti-Spyware * Anti-Malware * Anti-Spam			
9	Update status progress: Downloaded: 0.24 kB (0.00 kB/sec)			
Checking data	base integrity: OK	4		
Checking anti-spam database integrity: OK				
Signature database information100%				
Installed version: 331, current version: 331				
Signatures are	up-to-date.			
Anti-Spam database information100%				
☑ Installed version: 200, current version: 200				
Signatures are up-to-date.				
		Close		

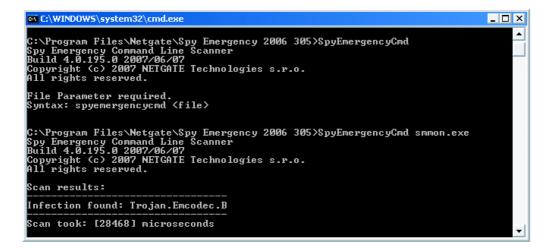
Automatic updates allows user to automatically update signature databases. When enabled Spy Emergency will check for new signatures at program startup and at regular interval specified by the update interval value.

To update manually press the **Update Now** button in the **Status** dialog.

Spy Emergency 2007 use incremental updates to minimize download times and speed up update process.

9. Command line interface

Command line interface allows user to scan files for threats from the command line. Command line utility is located in the Spy Emergency installation folder. Command line utility takes one file argument. Syntax is: SpyEmergencyCmd.exe <filename>.



10. Shell extension

Shell extension is a handy way to scan specific files or folders by right clicking on selected item in windows explorer window or in any file manager that support it. When popup is shown press the **Scan with Spy Emergency** option.

11. Technical support

Technical support team can be reached at <u>support@spy-emergency.com</u> or <u>support@netgate.sk</u> directly.

All other questions regarding sales or general information questions please direct to <u>netgate@netgate.sk</u>