MDaemon
AntiVirus

Alt-N Technologies, Ltd
1179 Corporate Drive West, #103
Arlington, TX 76006
Tel: (817) 652-0204

Contents

Abstract **3**

A Very Brief Summary of Computer Viruses **4**

Electronic Thugs with a Honorable Beginning 4
How Many Ways Can a Virus Attack? 4
The Cost of Viruses 5
The Email Doorway 5
Email AntiVirus Software 5
Deploying AntiVirus Software 6

MDaemon AntiVirus **7**

AntiVirus Design 7
AntiVirus Configuration and Update 9
AntiVirus Settings 9
AntiVirus Update 11
Kaspersky Engine 14
Virus Scanning Limitations and Suggestions 14

Abstract

Viruses cause billions of dollars (U.S.) of damage each year through downtime, lost productivity and recovery efforts. MDaemon AntiVirus is a complete virus checker with automated update capabilities for its scanning engine and virus signature files. When coupled with other preventative measures, MDaemon AntiVirus can reduce or, possibly, eliminate the encroachment of viruses into your office. It can also prevent the accidental sending of viruses from your business to other people. In addition to signature files, MDaemon AntiVirus uses heuristic detection methods, which examine emails and attachments for “virus-like” characteristics. MDaemon AntiVirus is a plug-in that runs as an independent service for Alt-N’s MDaemon email server.

A Very Brief Summary of Computer Viruses

Electronic Thugs with a Honorable Beginning

Computer viruses are programs and scripts designed to increase turmoil in the e-world. Virus writers bring many motivations to their work, including fame, pranks, curiosity, political statements, theft, vandalism and revenge. However, the first virus creators were mostly researchers and students learning how to manipulate the core memory of computer systems by playing predatory games. This practice has become formalized as a totally geek pastime called *Core Wars*.

```
         SPL     1.3
         MOV     }copy.>copy
         DJN     2.#1
         JMP     2434.#1
         MOV     }-10.>-10
copy     DAT     0.2430
jmpb     JMP     -2 . < -6
begin    MOV.I   splb . @ targ
         MOV.I   jmpb . # tartg
trag     MOV.I   -2430.@-2432
         ADD.F   inc.targ
         DJN     -4.#799
splb     SPL     0.4
         MOV     1.<-2
inc      DAT     }-2430.>-2430
```

The purpose of the game is having two or more programs compete against each other for access to memory. The objective is to control the memory and eliminate all competitor programs. The game emphasizes attack, defense, stealth and replication. This type of gaming gives software researchers skills in learning how to run multiple applications simultaneously on one computer. As an overflow, it helps in developing software for testing and troubleshooting memory. *Core Wars* type of programming has also spawned applications for fighting electronic crime.

While *Core Wars* and its like are useful for entertainment, education and applications, its methodologies are also being exploited to create tens of thousands of destructive programs and scripts. These intruders mostly target defenseless computer systems.

How Many Ways Can a Virus Attack?

In everyday discussions, *virus* refers to any program or script running without permission on a computer. Technically speaking, however, viruses are one of the three major electronic threats of this type. The other two are *worms* and *trojans*.

Viruses[1] are similar to parasites. They attach themselves to regular programs or scripts and become active when their hosts run. They replicate themselves by infecting other programs or scripts. Some viruses just spread while others cause harm or destroy computer resources, such as user documents and system files.

---

[1] For clarity, this document uses *virus* generically for *virus*, *worm* and *trojan*.

Worms are standalone programs or scripts. When run, they copy themselves to other directories and machines using network facilities. Like viruses, they may spread or do damage as they travel.

Trojans actually do one thing while masquerading as something else. They do not replicate or copy themselves, but spread when users share them across a network or through email. Trojans frequently damage system resources.

Some electronic predators mix the characteristics and capabilities of trojans, worms and viruses.

Viruses, worms and trojans can deliver jokes, but even these waste the time and energy of people and computers.

The Cost of Viruses

No one really knows the amount of economic losses resulting from harmful viruses. Several surveys show companies just deal with the problems and move on without counting the cost of system downtime, lost productivity and repair. Guesstimates are in the billions of U.S. dollars worldwide.

But whatever the losses, a little prevention can greatly reduce the risks and costs.

The Email Doorway

Email is the primary entry method viruses employ for gaining access to computers and networks. This is because email is innately open, convenient and effortless to use. It is also the most frequently applied tool on the Internet. By its design, email provides access to the business machines people use.

Once they are inside, viruses cause their damage and spread, typically using email as the transport.

Email AntiVirus Software

Because email is a primary access point for the spread of viruses, it is also the sensible place to post a guard in the form of anti-virus software.

Anti-virus software scans incoming emails and attachments for viruses. When it finds a virus, the software can delete or isolate the message. It can optionally notify the sender and receiver of the action.

Typically, the software recognizes viruses by looking for the “digital signature” each virus contains. This type of software uses a signature file of all known viruses. Signature files can be updated periodically, typically daily, to stay current with newly discovered viruses.

Some viruses use sophisticated masquerading technologies to alter their signatures, which makes signature detection more difficult. In addition, signature

files are seldom totally up-to-date because of the rapid introduction of new viruses.

To help discover and quarantine new and stealth viruses, some anti-virus software uses *heuristic* technology. Heuristics examine emails and attachments for “virus-like” code. For example, an attachment containing code for deleting all executable files might be tagged as a possible virus. The same label might apply to a script with the ability to modify the Windows registry.

Deploying AntiVirus Software

Anti-virus applications can be part of an email server or operate adjunct to it. As part of an email server, anti-viral software uses the server’s processing resources, which can dramatically slow down the sorting, sending and receiving of email.

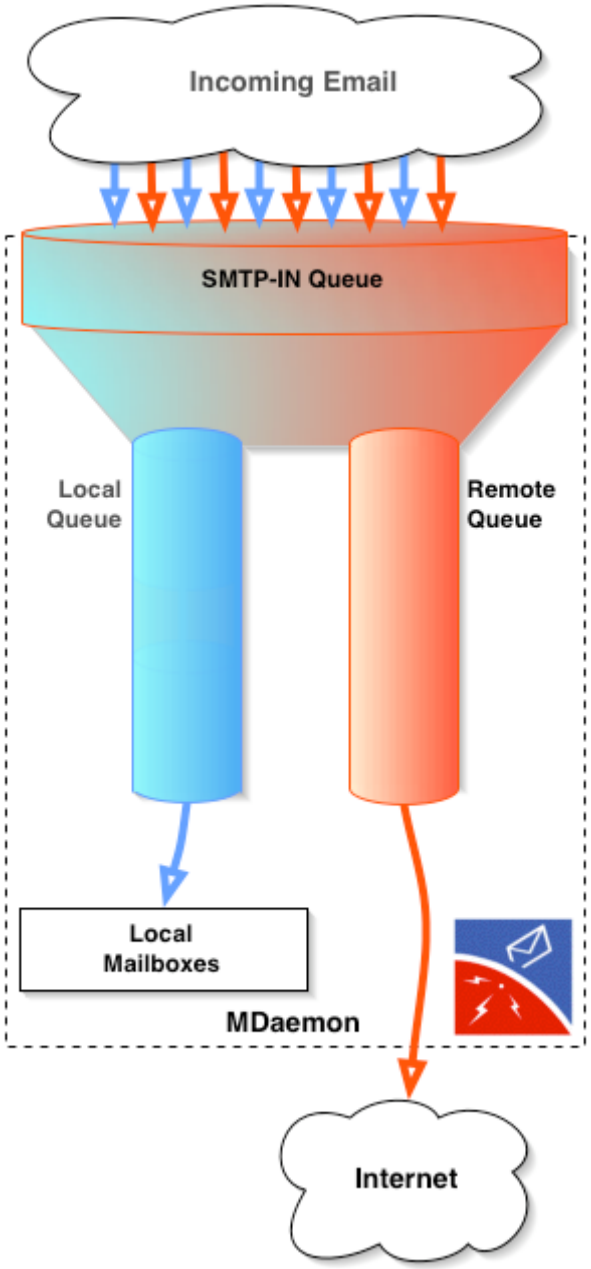
Adjunct applications operate alongside the email server without directly using its processing resources. If run on the same machine as the email server, adjunct software also slows down the machine, but does not impact the overall operation of email delivery as much as a built-in anti-virus solution.

MDaemon AntiVirus

AntiVirus Design

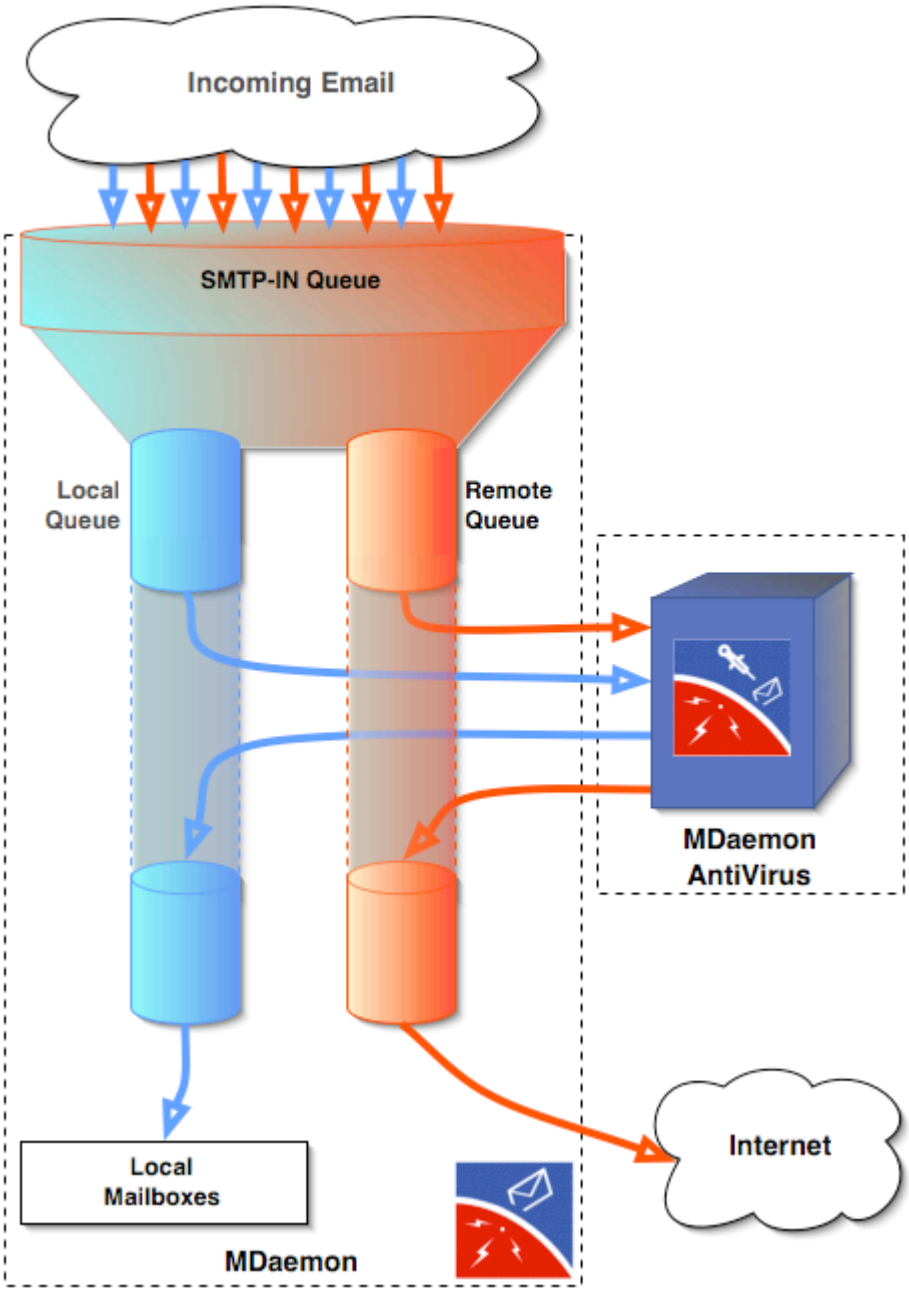
MDaemon AntiVirus is an email server plug-in which operates as an adjunct application. It runs separately and interacts only with the local and remote queues, but not the overall processing resources of MDaemon.

The illustration shows a simplified view of MDaemon's queues without anti-virus protection.



Incoming email is sorted into the local and remote queues. Mail for users with accounts on the email server goes into the local queue. All other mail goes into the remote queue and on to its Internet or other remote destinations.

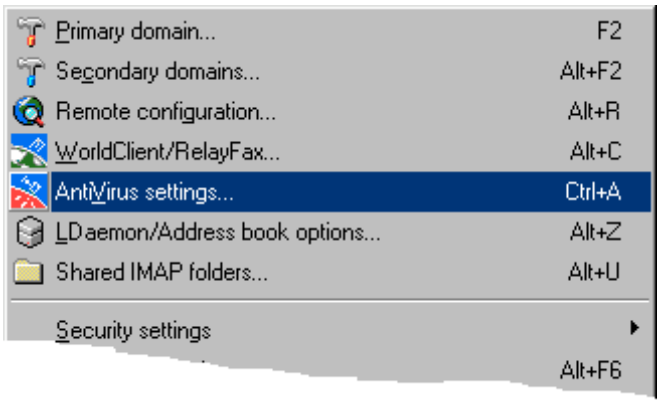
The next illustration shows MDaemon AntiVirus interacting with the queues.



Mail is moved out from the queues, processed by MDaemon AntiVirus, returned to the queues, then sent on to the local or remote destinations.

AntiVirus Configuration and Update

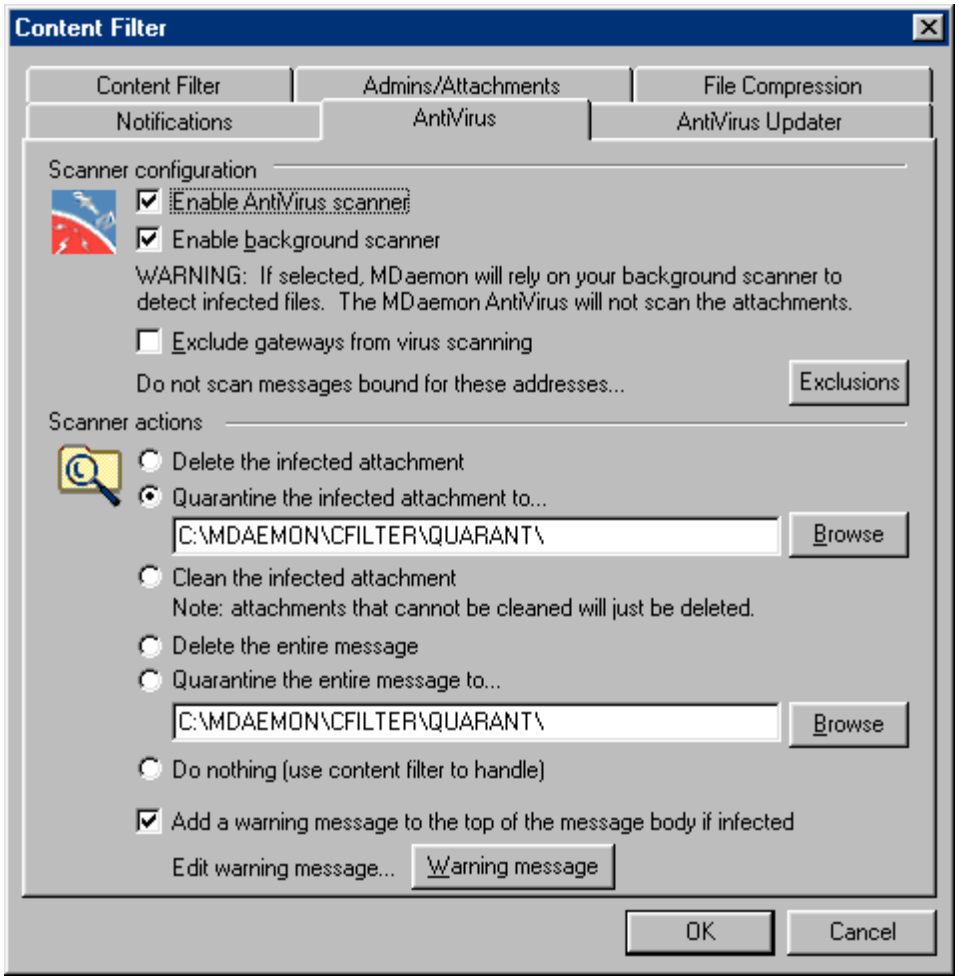
AntiVirus operates as part of MDaemon Content Filtering.



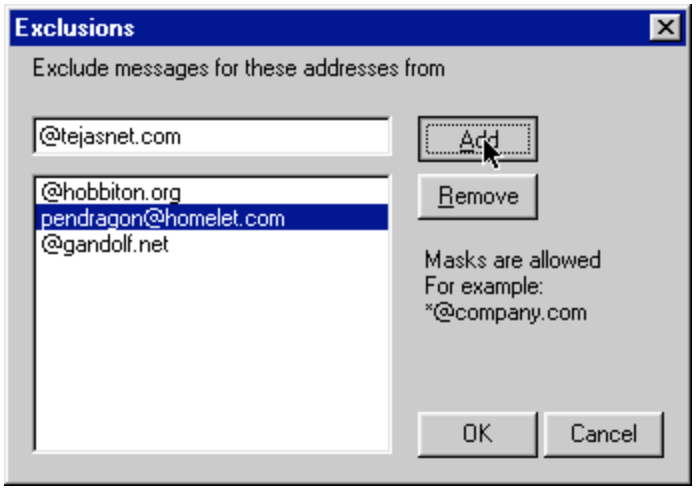
Selecting the **AntiVirus Settings** command from the **Setup** menu accesses tabs for configuring and updating AntiVirus.

AntiVirus Settings

Configuring AntiVirus is very easy. The illustration shows the setup dialog.

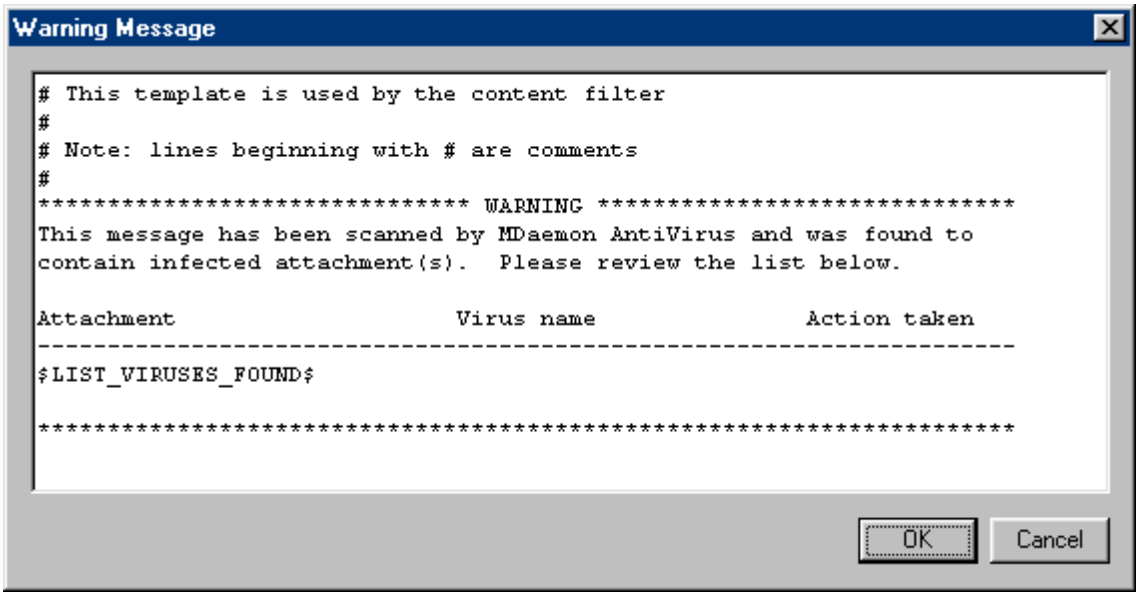


There are only seven settings for configuring MDaemon AntiVirus. Activating just one, the **Enable AntiVirus scanner** check box, starts virus protection for all domains. Specific addresses and domains can be excluded from scanning by using the **Exclusions** command button. All gateways can also be omitted through the **Exclude gateways…** check box. These three easy options supply enough flexibility to offer scanning as a *paid for* option. For example, an ISP could enable scanning, then exclude domains opting out. The next illustration shows the Exclusion dialog with several domains filled in.



Additional configuration options determine what to do with infected email or attachments. This includes alternatives such as deleting, quarantining or cleaning the virus.

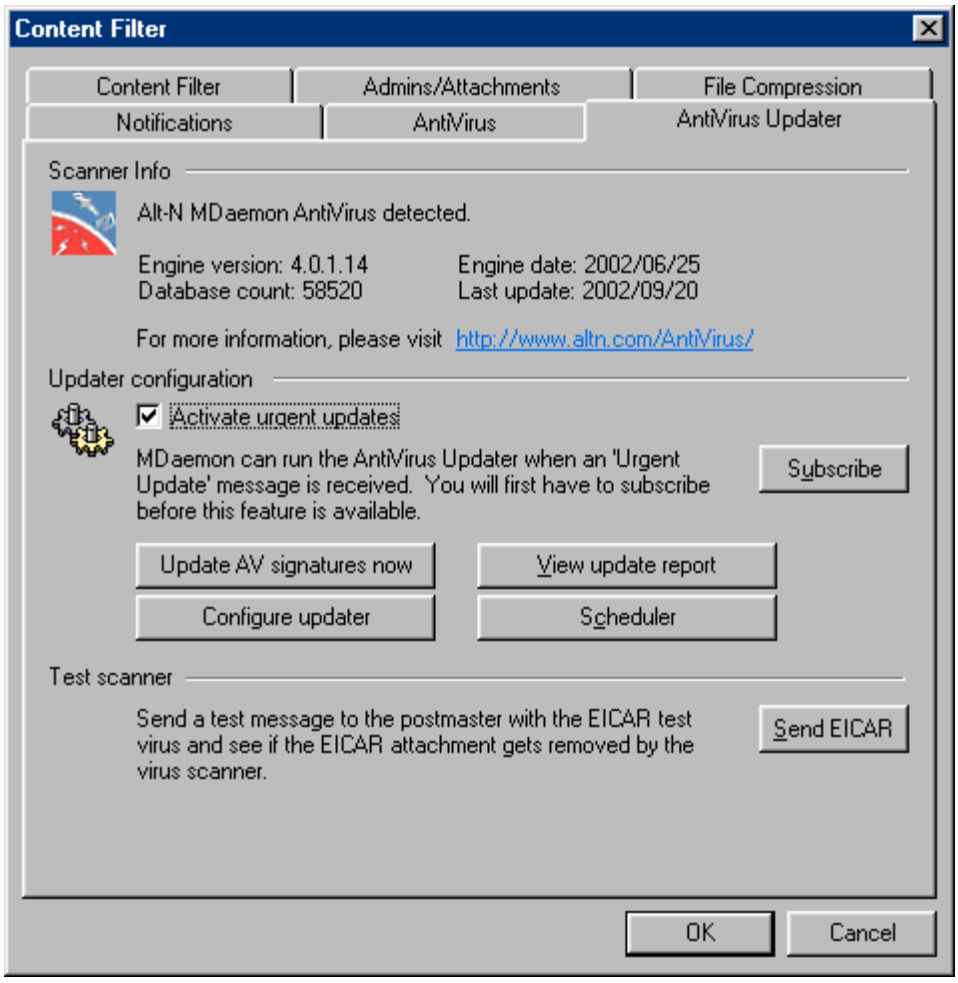
You can also activate and set up a message to transmit to the sender and intended receiver of the original infected message. The illustration shows a sample message:



AntiVirus Update

MDaemon AntiVirus is very easy to update. Both the scanning engine and the virus signature files can be updated manually or on an automatic schedule. There can be different schedules for normal and emergency updates. An emergency update might include the signature of a new, rapidly spreading and very damaging virus.

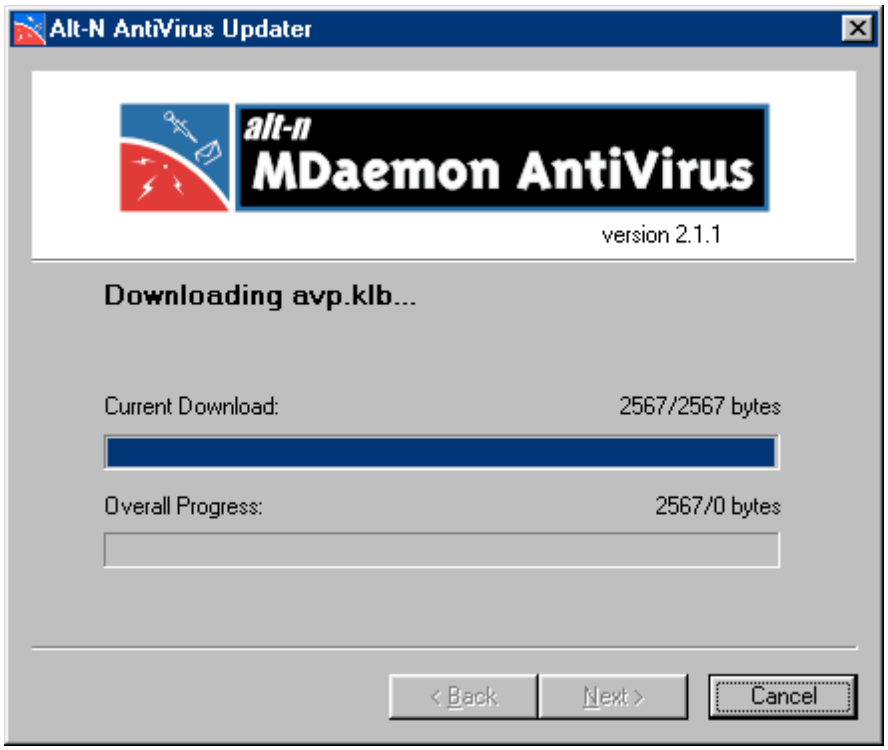
The illustration shows the dialog for configuring the updater.



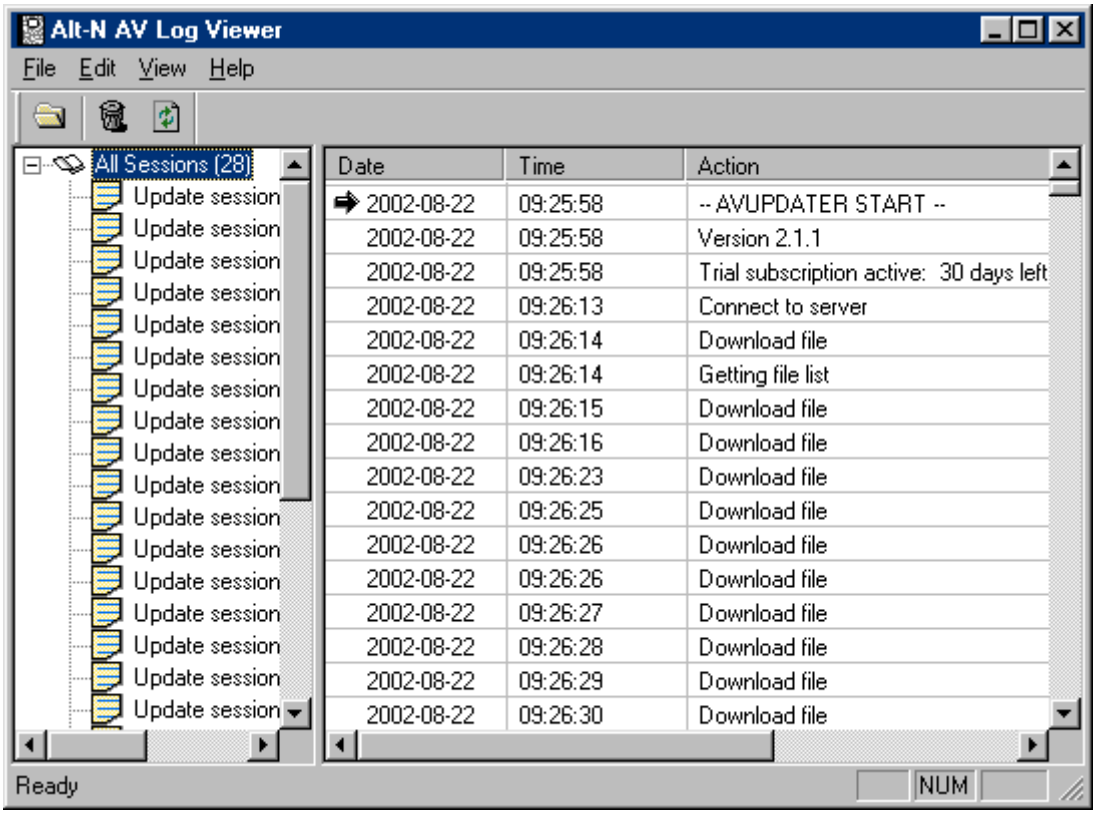
Options include a check box for enabling urgent updates. This is a free subscription available from the Alt-N website by using the **Subscribe** command button.

The configuration options include four command buttons:

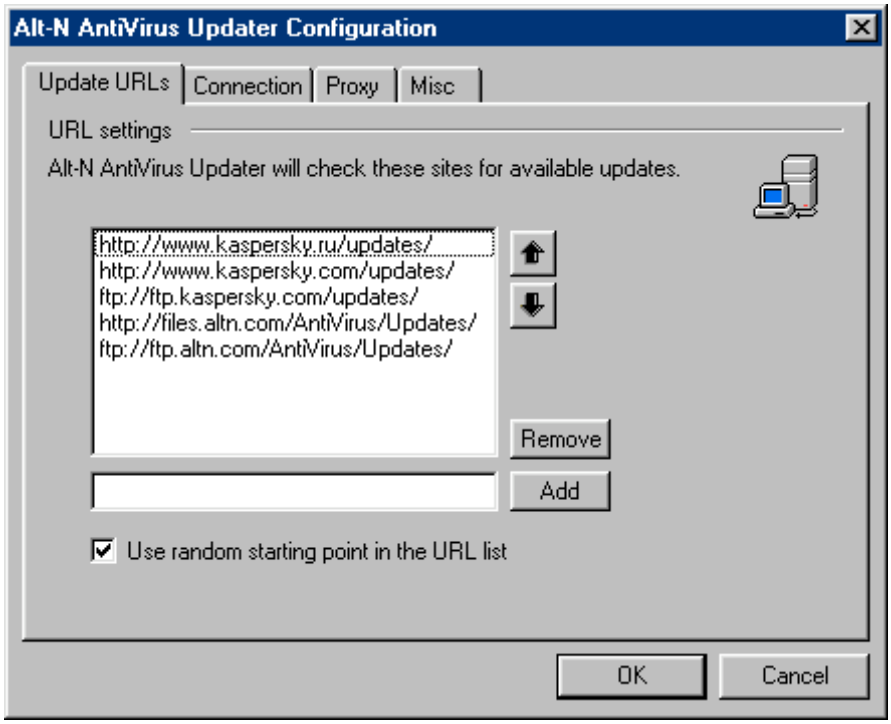
- **Update AV signature now**, for manually updating the signature file.



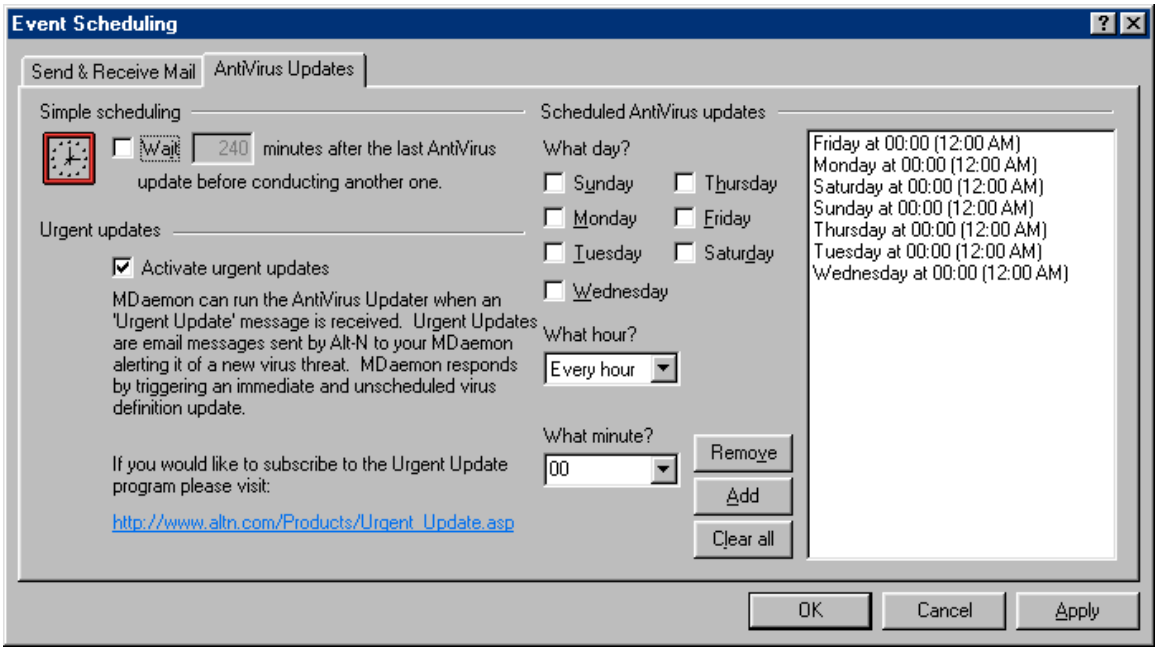
- **View Update report**, for viewing the automatic and manual update history.



- **Configure updater**, for setting up URL's and connection parameters for downloading updates.



- **Scheduler**, for configuring days and times for setting up automatic regular and emergency updates.



Kaspersky Engine

MDaemon AntiVirus is built on the Kaspersky virus scanning engine, developed by Kaspersky Labs, a Russian company. Although not as well-known as some of its competitor products, in recent comparative tests by several labs and publishing companies, the Kaspersky engine has earned positive reviews.

Virus Scanning Limitations and Suggestions

All virus scanning software is less than 100 percent reliable. This is because new viruses are always being introduced so signature files are usually somewhat behind.

In addition, virus writers are developing new ways to mask and distribute their viruses. For example, compressed and password protected files cannot be checked for viruses. Also, some viruses are starting to show up in java scripts and active server page scripts embedded in HTML emails. Some virus developers are even releasing test viruses with no payloads to see how they work in the real world. This is sort of like beta testing viruses before final release.

To further reduce the threat of virus attacks enterprises can:

- Block all executable attachments at the firewall or with content filtering. If a virus cannot get in, it cannot be executed.
- Block all data files containing macros, or remove the macros before delivering the files. This includes macro-enabled Word, PowerPoint and Excel files. These files can still be transmitted from one location to another using HTTP, FTP and email catalogs.
- Scan all HTML emails for scripts and remove the scripts before sending them on.
- Educate users about the risks of opening executable files received through email. This includes animated postcards, slide shows and the like.
- Disable automatic execution of scripts and programs received through email.
- Remove or disable the scripting engine for desktop users not required to have scripting available for work reasons.

Some of these suggestions may be politically difficult, but even partial implementation can help dry up the market for viruses. If the market goes away, the virus developers will have to find something else to do.