SMTP Gateway Virus Filtering with Sendmail and AMaViS

Kevin Swab

SMTP Gateway Virus Filtering with Sendmail and AMaViS

Kevin Swab

August 8th, 2001

GSEC Practical Assignment Version 1.2e

Introduction

We hear about it all too frequently - a new computer virus is spreading rapidly though the internet via e-mail causing widespread damage. Educating our users doesn't seem to be enough - clever social engineering and plain-old curiosity seem to get the better of people every time. While desktop anti-virus software can help, it isn't a cure-all. The anti-virus signatures may be out of date, or the software itself may have simply been turned off. As the number of desktops in an organization increases, maintaining their anti-virus software can seem like an impossible task.

An additional layer of defense is needed. Anti-Virus filtering at the SMTP gateway stops infected e-mail messages before they enter an organization, so they can do no harm. The case for filtering viruses at the gateway has been well presented by others. In "Anti-Virus Architecture: A 4-Layer Approach", Sobers states that "Virus Authors are currently using e-mail as the method of transmission. Most users will unwittingly open attachments and release the proverbial genie out of its bottle". In "The Case for an SMTP Gateway Anti-Virus System", Steen adds that "Relying on just one layer of virus defense, such as anti-virus software on the desktop, is like a bank with no locks or alarm system". For many organizations however, implementation of a commercial SMTP anti-virus solution may be cost prohibitive, or may require undesirable changes to system or network topology. This paper describes the software necessary for adding low-cost virus filtering capability to any UNIX / Sendmail SMTP gateway, details its installation and configuration, and relates some observations on its use.

Software

This solution is made possible by using a piece of open-source software called AMaViS (A Mail Virus Scanner). It acts as an interface between Sendmail (or another supported MTA) and an inexpensive commercial command-line virus scanning utility. AMaViS decomposes an e-mail into its constituent parts, decoding attachments, and uncompressing/unarchiving any files contained therein. The parts are then scanned by one or more supported virus scanning utilities. Infected messages are quarantined and alert messages are sent to a local administrator and to the original sender. Clean messages are delivered to their intended recipient(s) with a header similar to the following added:

```
X-Virus-Scanned: by AMaViS-perl11-milter (http://amavis.org/)
```

AMaViS supports e-mail encoded with the following schemes: MIME, uuencode, TNEF and BinHex, along with ordinary ASCII text. The following archival/compression file formats are also supported: .zip, .Z, .gz, .tar, .zoo, .F, .arc, .arj, .bz2, .lha, and .rar, along with self-extracting versions of many of the above. Archived/Compressed files can be nested up to a user-definable depth (the default is 20). AMaViS was developed by Mogens Kjaer, Christian Bricart, Rainer Link and others, and can be acquired from http://amavis.org.

A visit to the AMaViS web site will reveal that there are several releases of AMaViS available. The old stable release, AMaViS 0.2.1 is a shell script which relies heavily on external programs for its functionality. The current stable release is AMaViS-perl-11 - a rewrite in perl, which greatly reduces the dependence on external programs, and simplifies installation. This release can also be used in conjunction with the "milter" interface introduced in Sendmail 8.10. There is also an "amavisd" development branch, which will run as a daemon. Because a daemon would eliminate the overhead associated with launching perl for each scanned message, this looks like the best approach, but cautious sites may want to wait for a stable release.

In its most basic configuration AMaViS takes the place of the local delivery agent in the send-mail.cf file. When Sendmail decides to deliver a message locally, it calls AMaViS instead of the local delivery agent. If AMaViS ok's the message, it calls the local delivery agent directly to deliver the message. Note that in this configuration, only incoming mail is scanned - outgoing and relayed mail is sent without intervention. Sendmail can be made to scan outgoing and relayed mail, but that configuration requires complex changes to the sendmail.cf file[1].

A better solution is to take advantage of the "milter" interface present in sendmail versions 8.10 and above. Milter is Sendmail's new standard interface for filtering e-mail, and AMaViS-perl provides the option use it. The changes required to the sendmail configuration are minimal, and all incoming, outgoing, & relayed mail are scanned.

Building and Installing the Software

Our site has chosen to run AMaViS-perl11-milter. We run Sendmail 8.11.4 on a Solaris 7 system, but the setup should be portable to any modern UNIX / Sendmail configuration. Note that the following procedure will require building software packages from their source distributions, and re-configuring sendmail. If you are unfamiliar with building software from source, please have a look at the "Software Building-HOWTO" from the Linux Documentation Project. Although it's written for Linux, much of the content applies to any UNIX-like operating system. For Help with sendmail configuration, see "Sendmail Configuration Files", by Sendmail creator Eric Allman.

While AMaViS-perl greatly reduces its predecessor's dependence on external programs through the use of perl modules, there are still a few required. Aside from the obvious (Sendmail, Perl, and a supported virus scanner), these programs are also required:

- file - an enhanced "file" command capable of distinguishing many different file formats.
- arc - for extracting .arc archives
- bunzip2 - for uncompressing .bz2 files (Bundled with Solaris 8)
- lha - for extracting .lha archives
- unarj - for extracting .arj archives
- uncompress - for uncompressing .Z files (Bundled with most UNIX-like operating systems)
- unrar - for extracting .rar archives
- zoo - for extracting .zoo archives

If any of these are missing from your system, you'll need to locate either pre-compiled binaries for your OS, or build them from source code yourself. The file "doc/amavis.txt" in the AMaViS distribution directory lists locations where source code is available. For Solaris, precompiled binaries for some of the programs are available at http://sunfreeware.com.

Additionally, a list of perl modules available from CPAN (Comprehensive Perl Archive Network - http://www.cpan.org) is required. The "README" file in the AMaViS distribution directory describes the following simple procedure for installing the required modules:

> If you have the CPAN module installed, the most convenient way to install these modules is to launch the CPAN shell with
>
> ```
> perl -MCPAN -e shell
> ```
>
> and tell it to:
>
> ```
> install Unix::Syslog
> install Convert::UUlib
> install Convert::TNEF
> install Compress::Zlib
> install Archive::Tar
> install Archive::Zip
> install G/GB/GBARR/MailTools-1.15.tar.gz
> install MIME::Tools
> install Bundle::libnet
> ```
>
> The CPAN shell will automatically install modules which are required by those you requested (e.g. MIME-Base64, required by MIME-tools), and it also takes care of updating older modules.

If Perl itself is not installed on your system, it is also available from CPAN.

In order to install the "milter" version of AMaViS-perl, you'll first need a milter-enabled sendmail. As of release 8.11.4, milter is designated as "FFR" - For Future Release. This means that the milter functionality isn't compiled in by default, so you'll most likely need to rebuild sendmail with milter support turned on - From "Filtering Mail with Sendmail - Installation and Configuration" (Sendmail Inc)

> First, you must compile sendmail versions before 8.12 with _FFR_MILTER defined. To do this, add the following lines to your build configuration file (devtools/Site/config.site.m4)
>
> ```
> APPENDDEF('conf_sendmail_ENVDEF', '-D_FFR_MILTER=1')
> APPENDDEF('conf_libmilter_ENVDEF', '-D_FFR_MILTER=1')
> ```
>
> then type "`./Build -c`" in your sendmail directory.

If you've been using the sendmail binary delivered with your OS, you'll need to get the sendmail source code from http://www.sendmail.org.

The milter-enabled sendmail process communicates with AMaViS through a daemon process called "amavis-milter". To ensure that it builds correctly, Follow these instructions from the "README.milter" file in the AMaViS distribution directory:

> To compile the amavis-milter client, configure must be able to find the libmilter includes and libraries. The milter libraries (libmilter,libsmutil) must be installed where the linker can find them. If the libmilter includes are not in the compiler's include search path, their location can be passed to configure using --with-sendmail-source=DIR, where DIR is the sendmail source directory. configure will then add DIR/include to the include file search path.

Also note that "amavis-milter" must be started before sendmail, so after installation is complete, you'll need to modify your system startup scripts appropriately.

Once all the prerequisite software is in place, building and installing AMaViS is relatively straightforward. First, create an e-mail alias for "virusalert" - this is where AMaViS will send alert messages. Next, run "configure" with the appropriate arguments. If your system is like most, it probably already had a "file" command. You may have chosen to install the enhanced "file" command required by AMaViS in an alternate location. If so, include the "--with-file" switch on the configure line, along with a few other appropriate arguments:

```
./configure --with-file=(path to enhanced file command) \
--with-sendmail-source=(path to sendmail src directory) \
--enable-milter
```

Once configure completes successfully, you can type "make" followed by "make check". The check will test AMaViS against a sample file that contains the eicar.com[2] test file, which has been MIME encoded and nested inside multiple archive file formats. If "make check" was successful, you can install AMaViS with a "make install".

Once installation is complete, you can proceed to modifying your Sendmail configuration. This can be accomplished either by directly editing the sendmail.cf file, or by adding a few lines to your M4 configuration file and generating a new sendmail.cf from it. From "README.milter" in the AMaViS distribution directory:

> [...] add the following to sendmail.cf
>
> in the options section:
> O InputMailFilters=milter-amavis
>
> and in the mailers section at the bottom:
> Xmilter-amavis, S=local:/var/amavis/amavis.sock, T=S:10m;R:10m;E:10m
>
> If you prefer the m4 approach, add
> define('_FFR_MILTER', '1')dnl
> INPUT_MAIL_FILTER('milter-amavis', 'S=local:/var/amavis/amavis.sock,
> T=S:10m;R:10m;E:10m')dnl
>
> to your .mc file.

Now it's time to try things out - Start "amavis-milter" as specified in "README.milter":

```
rm -rf /var/amavis/amavis.sock
nohup /usr/sbin/amavis-milter -p local:/var/amavis/amavis.sock&
```

Once "amavis-milter" is running, stop and restart sendmail with your new configuration file in place. To test the new setup, retrieve a copy of the EICAR test file from http://www.eicar.org and mail it to yourself. With any luck, the message won't be delivered, instead, the sender (you) will receive an e-mail explaining that a message you sent was found to contain a virus, and the administrator (you) will receive a message stating that a virus-infected message has been quarantined in a specified directory, which defaults to /var/virusmails.

AMaViS in Use

AMaViS has been in place on our network since February 12th, 2001 (version 0.2.1, switching to AMaViS-perl11-milter in early June) and has worked flawlessly during that time. Coincidentally, February 12th happened to be the date that VBS/OnTheFly (aka: AnnaKournikova.jpg.vbs) was propagating through our organization - AMaViS blocked its first message about 60 seconds after coming online. Since then, it has handled each new outbreak in stride, the most recent example being the SirCam virus.

Our server only handles about 300 messages per day and to date there has been no noticeable performance impact as a result of running AMaViS. There may however be some performance issues to consider for a larger site. AMaViS creates a lot of temporary files, and necessitates some additional memory and CPU capacity. That being said, posters to the "amavis-user" mailing list have reported success with sites handling a very large volume of e-mail. Performance issues would be a consideration with any SMTP gateway anti-virus system, and should not deter you from considering AMaViS.

Using AMaViS is an easy decision to make for small to medium sites, and with adequate hardware and proper configuration, should be considered even for high volume mail servers. However, it's not a complete solution - Desktop anti-virus and user education are still important, as are secure SMTP server practices, such as denial of open relaying, and filtering out dangerous attachment types. We've shown how AMaViS can easily be integrated with an existing Sendmail SMTP gateway, giving an added layer of protection for a robust defense against e-mail borne viruses.

Notes:

1) See "README.sendmail" in the AMaViS distribution directory

2) European Institute for Computer Anti-Virus Research - Anti-Virus test file.

References:

Steen, Eric. “The Case for an SMTP Gateway Anti-Virus System”. SANS Information Security Reading Room. March 9th, 2001. URL: http://www.sans.org/infosecFAQ/email/SMTP.htm (August 8th, 2001)

Sobers, Larry. “Anti-Virus Architecture: A 4-Layer Approach”. SANS Information Security Reading Room. October 31st, 2000. URL: http://www.sans.org/infosecFAQ/malicious/anti-virus.htm (August 8th, 2001)

Steven M. Christensen and Associates, Inc. “Solaris Freeware Project”. URL: http://sunfree-ware.com (August 15th, 2001)

CPAN - Comprehensive Perl Archive Network. URL: http://www.cpan.org (August 9th, 2001)

“Filtering Mail with Sendmail - Installation and Configuration”. Sendmail Inc Home Page. 2000. URL: http://www.sendmail.com/partners/resources/development/milter-api/installation.html (August 8th, 2001)

Allman, Eric. “Sendmail Configuration Files”. Sendmail Home Page. February 2nd, 1999. URL: http://www.sendmail.org/m4/readme.html (August 8th, 2001)

Cooper, Mendel. “Building and Installing Software Packages for Linux”. The Linux Documenta-tion Project. July 27th, 1999. URL: http://www.linuxdoc.org/HOWTO/Software-Building-HOWTO.html (August 8th, 2001)

European Institute for Computer Anti-Virus Research. “EICAR Test File”. URL: http://www.eicar.org/anti_virus_test_file.htm (August 9th, 2001)

“amavis-user”. Mailing List Archives. URL: http://marc.theaimsgroup.com/?l=amavis-user&r=1&w=2 (August 9th, 2001)