ClamAVPlugin

The ClamAV Plugin

This plugin submits the entire email to a locally running Clam AntiVirus server for virus detection. If a virus is found, it returns a positive return code to indicate spam and sets the header "X-Spam-Virus: Yes ($virusname)".

Code

clamav.cf:

```
loadplugin ClamAV clamav.pm
full CLAMAV eval:check_clamav()
describe CLAMAV Clam AntiVirus detected a virus
score CLAMAV 10
add_header all Virus _CLAMAVRESULT_
```

clamav.pm:

```
package ClamAV;
use strict;

# version 2.0, 2010-01-07
#   - use SA public interface set_tag() and add_header, instead of
#     pushing a header field directly into $conf->{headers_spam}

# our $CLAMD_SOCK = 3310;               # for TCP-based usage
our $CLAMD_SOCK = "/var/run/clamd.basic/clamd.sock";   # change me

use Mail::SpamAssassin;
use Mail::SpamAssassin::Plugin;
use Mail::SpamAssassin::Logger;
use File::Scan::ClamAV;
our @ISA = qw(Mail::SpamAssassin::Plugin);

sub new {
  my ($class, $mailsa) = @_;
  $class = ref($class) || $class;
  my $self = $class->SUPER::new($mailsa);
  bless($self, $class);
  $self->register_eval_rule("check_clamav");
  return $self;
}

sub check_clamav {
  my($self, $pms, $fulltext) = @_;
  dbg("ClamAV: invoking File::Scan::ClamAV, port/socket: %s", $CLAMD_SOCK);
  my $clamav = new File::Scan::ClamAV(port => $CLAMD_SOCK);
  my($code, $virus) = $clamav->streamscan(${$fulltext});
  my $isspam = 0;
  my $header = "";
  if (!$code) {
    my $errstr = $clamav->errstr();
    $header = "Error ($errstr)";
  } elsif ($code eq 'OK') {
    $header = "No";
  } elsif ($code eq 'FOUND') {
    $header = "Yes ($virus)";
    $isspam = 1;
    # include the virus name in SpamAssassin's report
    $pms->test_log($virus);
  } else {
    $header = "Error (Unknown return code from ClamAV: $code)";
  }
  dbg("ClamAV: result - $header");
  $pms->set_tag('CLAMAVRESULT', $header);
  # add a metadatum so that rules can match against the result too
  $pms->{msg}->put_metadata('X-Spam-Virus',$header);
  return $isspam;
}

1;
```

How To Use It

First of all, you need to install ClamAV and ensure that scanning a mail with **clamscan** works.

Second, you need to install the File::Scan::ClamAV perl module.

Finally, save the two files above into the /etc/mail/spamassassin/ directory. You can adjust the default score of 10 in **clamav.cf** if you like. You should edit the **clamav.pm** file and change the setting for '$CLAMD_SOCK' to match where your ClamAV installation has put its named pipe.

Restart the spamd daemon if you're using that, and you should be all set.

If you'd like to sort virus emails to a separate folder, create a rule looking for the "X-Spam-Virus: Yes" header.

To get a different score based on virus type, see ClamAVMultipleScores.

Caveats

Some find this plugin very useful. However others do have a different opinion of the safety or logic of such a plugin that you should probably read – Andrew Ferrier

actually, having a plugin that does this, rather than building support directly into the core, is exactly what the "others" in question preferred 😉. So this is good – JustinMason

Very true 🙂 I have to say my experiences with this plugin so far have been very promising, I can recommend it to anyone suffering from the increasingly blurred distinction between spam and viruses. – AndrewFerrier