RelayCountryPlugin

Using the RelayCountry plugin

The RelayCountry plugin exposes the countries that a mail was relayed from – turn it on by reading that documentation page, installing the required CPAN module (see below), and uncommenting the 'loadplugin' line in the `/etc/mail/spamassassin/init.pre` file for `Mail::SpamAssassin::Plugin::RelayCountry`.

Required CPAN module dependencies, choose one:

GeoIP2::Reader::Database	Supported since SpamAssassin 3.4.2, install MaxMind::DB::Reader::XS for best performance
IP::Country::DB_File	Supported since SpamAssassin 3.4.2
Geo::IP	Supported since SpamAssassin 3.4.0
IP::Country::Fast	Not recommended, outdated

Country metadata will also be added to the Bayesian filtering process, allowing it to learn information based on countries.

You can also write rules that match specific countries and add them to your `/etc/mail/spamassassin/local.cf` file. For example:

```
header          RELAYCOUNTRY_BAD X-Relay-Countries =~ /CN/
describe        RELAYCOUNTRY_BAD Relayed through China at some point
score           RELAYCOUNTRY_BAD 3.0

header          RELAYCOUNTRY_GOOD X-Relay-Countries =~ /^(FI|SE)/
describe        RELAYCOUNTRY_GOOD First untrusted relay is Finland or Sweden :-)
score           RELAYCOUNTRY_GOOD -0.2
```

A list of 2-letter ISO 3166 country codes can be found from https://en.wikipedia.org/wiki/ISO_3166-1_alpha-2. Note that the plugin itself adds few special types: private IPs are marked with '**' (two asterisks) and IPs not found in database are marked with 'XX'.

You can find a list of countries that statistically relay most spam for example from http://www.spamhaus.org/statistics/countries.lasso. Be careful not to score too much or too many, email is global by nature.

It's also possible to add a separate MIME header that shows all the message's relay countries, independent of the rules:

```
add_header all Relay-Country _RELAYCOUNTRY_
```

This will show up in your MIME headers as:

```
X-Spam-Relay-Country: US CN RU
```

Note about GeoIP2::Reader::Database and Geo::IP

Perhaps the easiest to install, since most distributions package these.

Note that Geo::IP updates are discontinued since April 2018, so you should use the new GeoIP2 (MMDB) databases. Free and commercial versions can be found from several vendors:

https://dev.maxmind.com/geoip/geoip2/geolite2/

https://db-ip.com/db/lite.php

UPDATE: Maintained legacy Geo::IP databases can be downloaded from several 3rd party sites:

- https://mailfud.org/geoip-legacy/
- https://www.miyuru.lk/geoiplegacy

Note about IP::Country::DB_File

This module does not come with a database or update mechanism, but it is quite easy and fast to create yourself (it does need a bit of hacking, mentioned urls are outdated).

Here you can download occasionally updated files:

- https://mailfud.org/ip-country-dbfile/

The gunzipped file can be placed anywhere, just let SpamAssassin know where it is (country_db_path setting).

Note about IP::Country::Fast

As of writing, the latest included database is from 2013. There is no internal update mechanism.

The database consists of files named *cc.gif* and *ip.gif*. You can find the path with this command:

```
$ perl -MIP::Country::Fast -e '$_=$INC{"IP/Country/Fast.pm"};s/\.pm/\n/;print';
```

Updating the database files requires entering dbmScripts directory in IP::Country::Fast sources and running *whois_filenames*, *ipcc_loader.pl* and *ipcc_maker.pl* scripts in that order. Note that the build can use up to 2GB of system memory. The files must be put in directory mentioned above, it is not configurable.

Here you can download occasionally updated files:

- https://mailfud.org/ip-country-fast/