ClamAVMultipleScores

If you have deployed ClamAVPlugin and now you want to get a different score based on threat type, you can replace your **clamav.cf** with the following version.

Security Warning

Note that, since ClamAV reports only one threat type for each email even if the email has more threats, if you assign different scores to different threats you could only get the lowest score of these threats, leading to email bypass! For example, if you set a score of 20.0 to virus and a score of 2.0 to MSRBL and an email has both, you could get only the 2.0 score!

Score should take in account ClamAV priorities:

- phishing signatures have a higher priority than phishing heuristics;
- **TODO:** find and add other priorities in ClamAV.

Code

clamav.cf:

```
loadplugin ClamAV clamav.pm
full CLAMAV eval:check_clamav()
describe CLAMAV Clam AntiVirus detected something...
score CLAMAV 0.001

# Look for specific types of ClamAV detections
header __CLAMAV_PHISH X-Spam-Virus =~ /Yes.{1,30}Phishing/i
header __CLAMAV_PHISH_HEUR X-Spam-Virus =~ /Yes.{1,30}Phishing\.Heuristics\.Email/
header __CLAMAV_SANE X-Spam-Virus =~ /Yes.{1,30}Sanesecurity/i
header __CLAMAV_MBL X-Spam-Virus =~ /Yes.{1,30}MBL/
header __CLAMAV_MSRBL X-Spam-Virus =~ /Yes.{1,30}MSRBL/
header __CLAMAV_VX X-Spam-Virus =~ /Yes.{1,30}VX\./

# Give the above rules a very late priority so that they can see the output
# of previous rules - otherwise they don't work! Not sure what the correct
# priority should be but this seems to work...
priority __CLAMAV_PHISH 9999
priority __CLAMAV_PHISH_HEUR 9999
priority __CLAMAV_SANE 9999
priority __CLAMAV_MBL 9999
priority __CLAMAV_MSRBL 9999
priority __CLAMAV_VX 9999


# Work out what ClamAV detected and score accordingly

# ClamAV general signatures
meta CLAMAV_VIRUS (CLAMAV && !__CLAMAV_PHISH && !__CLAMAV_SANE && !__CLAMAV_MBL && !__CLAMAV_MSRBL && !
__CLAMAV_VX)
describe CLAMAV_VIRUS Virus found by ClamAV default signatures
score CLAMAV_VIRUS 20.0

# ClamAV phishing signatures
meta CLAMAV_PHISH (CLAMAV && __CLAMAV_PHISH && !__CLAMAV_SANE && !__CLAMAV_PHISH_HEUR)
describe CLAMAV_PHISH Phishing email found by ClamAV default signatures
score CLAMAV_PHISH 10.0

# ClamAV phishing with heuristic engine (not signatures based, may lead to false positives)
# Available since ClamAV 0.91
meta CLAMAV_PHISH_HEUR (CLAMAV && __CLAMAV_PHISH_HEUR)
describe CLAMAV_PHISH_HEUR Phishing email found by ClamAV heuristic engine
score CLAMAV_PHISH_HEUR 2.0

# ClamAV SaneSecurity signatures from http://www.sanesecurity.com/clamav/
meta CLAMAV_SANE (CLAMAV && __CLAMAV_SANE)
describe CLAMAV_SANE SPAM found by ClamAV SaneSecurity signatures
score CLAMAV_SANE 7.5

# ClamAV MBL signatures from http://www.malware.com.br/
meta CLAMAV_MBL (CLAMAV && __CLAMAV_MBL)
describe CLAMAV_MBL Malware found by ClamAV MBL signatures
score CLAMAV_MBL 7.5

# ClamAV MSRBL signatures from http://www.msrbl.com/
meta CLAMAV_MSRBL (CLAMAV && __CLAMAV_MSRBL)
describe CLAMAV_MSRBL SPAM found by ClamAV MSRBL signatures
score CLAMAV_MSRBL 2.0

# ClamAV SecuriteInfo.com VX malware signatures from
# http://www.securiteinfo.com/services/clamav_unofficial_malwares_signatures.shtml
meta CLAMAV_VX (CLAMAV && __CLAMAV_VX)
describe CLAMAV_VX Malware found by SecuriteInfo.com VX signatures
score CLAMAV_VX 5.0
```