Creating signatures for ClamAV

1 Introduction

CVD (ClamAV

That's it! The signature is ready to use:

```
zolw@localhost:/tmp/test$ clamscan -d test.hdb test.exe
test.exe: test.exe FOUND

----------- SCAN SUMMARY -----------
Known viruses: 1
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.02 MB
I/O buffer size: 131072 bytes
Time: 0.024 sec (0 m 0 s)
```

You can edit it to change the name (by default sigtool uses the file name). Remember that all MD5 signatures must be placed in `*.hdb` files, you can include any number of sigs in a file. To get them automatically loaded every time clamscan/clamd starts just copy them to local virus database directory.

3 signatures

ClamAV keeps viral fragments in

- `*`
  Match any number of bytes.

- `{n}`
  Match n bytes.

- `{-n}`
  Match n or less bytes.

- `{n-}`
  Match n or more bytes.

- `(a|b)`
  Match a and b (you can use more alternate characters).

3.3 Basic signature format

The simplest signatures are of the format:

```
MalwareName=HexSignature
```

ClamAV will analyse a whole content of a file trying to match it. All signatures of this type must be placed in `*.db`

```
sigtool --build daily.cvd --server SIGNING_SERVER
```

where SIGNING_SERVER is one of the ClamAV Signing Servers you have access to. This command will automatically generate binary database with a digital signature.

```
LibClamAV debug:
```

Please consult [1] for more information. After an update please send a summary to clamav-virusdb@lists.sf.net. Thanks!

References

[1] Luca Gibelli: *Mirroring the Virus Database*
http://www.clamav.net/doc/mirrors