1. Giới thiệu

CVD ( clamAV virus Database ) là một tệp tập hợp chữ ký số chứa một hoặc nhiều cơ sở dữ liệu. Phần header là một chuỗi dài 512 byte với các phần ngăn cách bởi dấu “hai chấm” :

ClamAV-VDB:build time:version:number of signatures:functionality level required:MD5 checksum:digital signature:builder name:build time (sec)

Thông tin chi tiết của tệp CVD

zolw@localhost:/usr/local/share/clamav$ sigtool -i daily.cvd

Build time: 11 Sep 2004 21-07 +0200

Version: 487

# of signatures: 1189

Functionality level: 2

Builder: ccordes

MD5: a3f4f98694229e461f17d2aa254e9a43

Digital signature: uwJS6d+y/9g5SXGE0Hh1rXyjZW/PGK/zqVtWWVL3/tfHEnA17z6VB2IBR2I/OitKRYzmVo3ibU7bPCJNgi6fPcW1PQwvCunwAswvR0ehrvY/4ksUjUOXo1VwQlW7l86HZmiMUSyAjnF/gciOSsOQa9Hli8D5uET1RDzVpoWu/id

Verification OK.

Có 2 CVD trong clamAV là main.cvd và daily.cvd

1. Chữ ký MD5

Có 1 cách đơn giản để tạo chữ ký cho mã độc tĩnh là sử dụng MD5 checksums.