# 系统名称：交互式恶意代码特征查询系统

# 文档名称：数据库设计文档

## 描绘E-R图



## 建立数据表

1. 域名(domain)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| D\_ID | Int(12) | 域名ID | P | 自增 |
| D\_Name | Varchar(64) | 名称 |  | 不可为空 |
| D\_ Registrar | Varchar(32) | 注册者 |  | 不可为空 |
| D\_RA | Varchar(32) | 注册机构 |  | 不可为空 |
| D\_Mailbox | Varchar(64) | 注册邮箱 |  | 不可为空 |
| D\_Address | Varchar(128) | 地址 |  | 不可为空 |
| D\_Phone | Int(12) | 注册预留电话 |  | 不可为空 |
| D\_RT | Date | 注册时间 |  | 不可为空 |
| D\_OT | Date | 过期时间 |  | 不可为空 |
| D\_UT | Date | 更新时间 |  | 不可为空 |
| D\_SP | Varchar(64) | 域名服务商 |  | 不可为空 |
| D\_S | Varchar(64) | 域名服务器 |  | 不可为空 |
| T\_IDNumber | Varchar(32) | 病毒标签ID标号 | F | 可为空，各标号用’;’（英文分号）隔开，被标签表约束 |

1. 样本（sample）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P | 自增 |
| S\_FT | Varchar(32) | 文件类型 |  | 不可为空 |
| S\_Size | Varchar(16) | 样本大小 |  | 不可为空 |
| S\_MD5 | Varchar(64) | 样本MD5 |  | 不可为空 |
| S\_Sha1 | Varchar(64) | 样本Sha1 |  | 不可为空 |
| S\_Sha256 | Varchar(64) | 样本Sha256 |  | 不可为空 |
| S\_Sha512 | Varchar(64) | 样本Sha512 |  | 不可为空 |
| S\_Ssdeep | Varchar(64) | 样本ssdeep |  | 不可为空 |
| S\_Imphash | Varchar(64) | 样本imphash |  | 不可为空 |
| T\_IDNumber | Varchar(32) | 病毒标签ID标号 | F | 可为空，各标号用’;’（英文分号）隔开，被标签表约束 |

1. IP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| IP\_ID | Int(12) | IP的ID | P | 自增 |
| IP\_Info | Varchar(32) | IP的具体信息 |  | 不可为空 |
| T\_IDNumber | Varchar(32) | 病毒标签ID标号 | F | 可为空，各标号用’;’（英文分号）隔开，被标签表约束 |

1. 检测结果(result)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F | 不可为空 |
| R\_Software | Varchar(32) | 杀毒软件 | P | 不可为空 |
| R\_Result | Varchar(32) | 检测结果 | P | 不可为空 |

1. PE section

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F | 不可为空 |
| PES\_Name | Varchar(16) | name | P | 不可为空 |
| PES\_Address | Varchar(64) | Virtual Address |  | 不可为空 |
| PES\_Size | Varchar(16) | Virtual Size |  | 不可为空 |
| PES\_SRD | Varchar(16) | Size of Raw Data |  | 不可为空 |
| PES\_ Entropy | Varchar(32) | Entropy |  | 不可为空 |

1. PE import

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F | 不可为空 |
| PEI\_DllName | Varchar(32) | Dll文件名 | P | 不可为空 |

1. 操作文件(file)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F | 不可为空 |
| F\_Catalog | Varchar(32) | 文件目录 | P | 不可为空 |

1. 操作注册表(registry)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F | 不可为空 |
| R\_Catalog | Varchar(32) | 注册表目录 | P | 不可为空 |

1. 互斥体（mutex）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F | 不可为空 |
| M\_Object | Varchar(64) | 操作对象 | P | 不可为空(只有数字为操作失败，其他为成功) |

1. 病毒标签tag

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| T\_ID | Int(8) | 病毒标签ID | P | 自增 |
| T\_Name | Varchar(32) | 标签名称 |  | 不可为空 |

1. 进程（process）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F | 不可为空 |
| P\_Name | Varchar(64) | 进程名称 |  | 不可为空 |
| P\_Pid | Int(6) | 进程PID | P | 不可为空 |

1. 样本—域名（SD）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| S\_ID | Int(12) | 样本ID | P、F |  |
| D\_ID | Int(12) | 域名ID | P、F | D\_ID与P\_ID有一个为空 |
| IP\_ID | Int(12) | IP的ID | P、F | D\_ID与P\_ID有一个为空 |

1. 域名—IP(DI)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名称 | 数据类型 | 说明 | 约束 | 备注 |
| IP\_ID | Int(12) | IP的ID | P、F | 不可为空 |
| D\_ID | Int(12) | 域名ID | P、F | 不可为空 |
| DI\_Time | Date | 时间 |  |  |