

点Label

|  |  |  |
| --- | --- | --- |
| 类型 | 说明 | 数据库字段 |
| IP | IP类 | IP\_SCHEMA\_MALWARE |
| HOST | 域 | HOST\_SCHEMA\_MALWARE |
| URL | 被攻击对象的URL | URL\_SCHEMA\_MALWARE |
| FILE | 文件 | FILE\_SCHEMA\_MALWARE |
| DEPARTMENT | 部门 | DEP\_SCHEMA\_MALWARE |

边Label

|  |  |  |
| --- | --- | --- |
| 类型 | 说明 | 数据库字段 |
| IP->Department | IP隶属于某个部门 | IP\_TO\_DEP\_SCHEMA\_MALWARE |
| IP->IP（访问流） | 访问流 | ACCESS\_SCHEMA\_MALWARE |
| HOST->IP | 域名下有哪些IP | HOST\_TO\_IP\_SCHEMA\_MALWARE |
| IP->FILE | IP下载过哪些文件 | IP\_TO\_FILE\_SCHEMA\_MALWARE |
| FILE->URL | 这个文件是从哪个地址下载的 | FILE\_TO\_URL\_SCHEMA\_MALWARE |
| URL->IP | 这个地址对应的IP（感觉可以不要这一项） | URL\_TO\_IP\_SCHEMA\_MALWARE |
| IP->HOST | 这个IP向哪个HOST发送过DNS请求 | DNS\_REQ\_SCHEMA\_MALWARE |

点属性

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 类型 | | 属性 | 说明 | 数据库字段 | 例 | |
| IP | | IP\_ADD | IP地址 | IP\_ADD\_SCHEMA\_MALWARE |  | |
| COUNTRY | 国家 | COUNTRY\_SCHEMA\_MALWARE |  | |
| PROVINCE | 省份 | PROVINCE\_SCHEMA\_MALWARE |  | |
|  | | | | | |
| HOST | | HOST\_NAME | 域名 | DOMAIN\_NAME\_SCHEMA\_MALWARE |  | |
| INFO | 信息 | INFO\_SCHEMA\_MALWARE |  | |
|  | | | | | |
| URL | URL\_ADD | | 这个文件是从哪个地址下载的 | URL\_ADD\_SCHEMA\_MALWARE |  | |
| INFO | | 信息 | INFO\_SCHEMA\_MALWARE |  | |
|  |  | |  |  |  | |
| DEPARTMENT | DEP\_NAME | | 部门名 | DEP\_NAME\_SCHEMA\_MALWARE |  | |
| INFO | | 信息 | INFO\_SCHEMA\_MALWARE |  | |
|  |  | |  |  |  | |
| FILE | MD5 | | 文件MD5值 | MD5\_SCHEMA\_MALWARE |  | |
| INFO | | 信息 | INFO\_SCHEMA\_MALWARE |  | |
|  |  | |  |  |  | |

边属性

边属性

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 类型 | 属性 | 说明 | 数据库字段 | 例 |
| IP\_TO\_DEP\_SCHEMA\_MALWARE |  |  |  |  |
|  |  |  |  |  |
| ACCESS\_SCHEMA\_MALWARE | PORT\_SOURCE | 源端口 | PORT\_SOURCE\_SCHEMA\_MALWARE |  |
| PORT\_DST | 目的端口 | PORT\_DST\_SCHEMA\_MALWARE |  |
| PACKAGE\_NUM | 包数 | PACKAGE\_NUM\_SCHEMA\_MALWARE |  |
| BYTES | 字节数 | BYTES\_SCHEMA\_MALWARE |  |
| TIME | 时间 | TIME\_SCHEMA\_MALWARE |  |
| TCP\_FLAG | TCP标志 | TCP\_FLAG\_SCHEMA\_MALWARE |  |
| TRANS\_PROTO | 传输协议 | TRANS\_PROTO\_SCHEMA\_MALWARE |  |
| HASH | 哈希 | HASH\_SCHEMA\_MALWARE |  |
|  |  |  |  |  |
| HOST\_TO\_IP\_SCHEMA\_MALWARE |  |  |  |  |
|  |  |  |  |  |
| IP\_TO\_FILE\_SCHEMA\_MALWARE | TIME | 时间 | TIME\_SCHEMA\_MALWARE |  |
| Download\_Source\_IP | 从哪个IP下载的 | DSI\_SHCEME\_MALWARE |  |
| Download\_Source\_URL | 下载的URL | DSU\_SCHEMA\_MALWARE |  |
| HASH | 哈希 | HASH\_SCHEMA\_MALWARE |  |
|  | | | | |
| FILE\_TO\_URL\_SCHEMA\_MALWARE |  |  |  |  |
|  | | | | |
| URL\_TO\_IP\_SCHEMA\_MALWARE |  |  |  |  |
|  | | | | |
| DNS\_REQ\_SCHEMA\_MALWARE | DNS\_SERVER | 域名服务器 | DNS\_SERVER\_SCHEMA\_MALWARE |  |
| PROTOCOL | 协议（此处都是17） | PROTO\_SCHEMA\_MALWARE |  |
| REQ\_DOMAINNAME | 请求域名 | REQ\_DN\_SCHEMA\_MALWARE |  |
| REQ\_TYPE | 请求类型 | REQ\_TYPE\_SCHEMA\_MALWARE |  |
| REQ\_COUNT | 请求次数 | REQ\_COUNT\_SCHEMA\_MALWARE |  |
| DIRECTION | 方向 | DIRECT\_SCHEMA\_MALWARE |  |
| Authority response identifier | 权威应答标识 | ASI\_SCHEMA\_MALWARE |  |
| Answer | 应答值 | ANSWER\_SCHEMA\_MALWARE |  |
| RR\_REQ\_TYPE | RP请求类型 | RP\_REQ\_TYPE\_SCHEMA\_MALWARE |  |
| Resolution \_IP | 解析出的域名对应的IP | RS\_IP\_SCHEMA\_MALWARE |  |
| TTL | TTL | TTL\_SCHEMA\_MALWARE |  |
| TIME | 时间 | TIME\_SCHEMA\_MALWARE |  |
| SAMPLING\_RATE | 采样比 | SR\_SCHEMA\_MALWARE |  |
| HASH | 哈希 | HASH\_SCHEMA\_MALWARE |  |