|  |  |
| --- | --- |
| 编号 | 1 |
| 名称 | 获取与域名相关的威胁情报（即样本）（sd）Get\_domainSample |
| 输入 | 域名ID |
| 输出 | 与查询样本相关的所有样本 |

|  |  |
| --- | --- |
| 编号 | 2 |
| 名称 | 获取最近与域名有联系的IP(di)Get\_domainIP |
| 输入 | 域名ID |
| 输出 | Ip\_info |

|  |  |
| --- | --- |
| 编号 | 3 |
| 名称 | 获取指向最近与域名有联系的IP的域名数量(di,sd)Get\_domainIPNum |
| 输入 | IP\_ID,域名ID |
| 输出 | 域名总数 |

|  |  |
| --- | --- |
| 编号 | 4 |
| 名称 | 获取域名的解析记录(di)Get\_domainRecord |
| 输入 | 域名ID |
| 输出 | All解析记录 |

|  |  |
| --- | --- |
| 编号 | 5 |
| 名称 | 获取指向与域名有联系的IP的域名列表(di,sd)Get\_domainIPDomainList |
| 输入 | 域名ID、IP\_ID |
| 输出 | 域名列表 |

|  |  |
| --- | --- |
| 编号 | 6 |
| 名称 | 获取子域名(dd)Get\_childrenDomain |
| 输入 | 域名ID |
| 输出 | 子域名列表 |

|  |  |
| --- | --- |
| 编号 | 7 |
| 名称 | 获取父域名（dd）Get\_fatherDomain |
| 输入 | 域名ID |
| 输出 | 父域名 |

|  |  |
| --- | --- |
| 编号 | 8 |
| 名称 | 获取whois信息（domain）Get\_domainWhois |
| 输入 | 域名ID |
| 输出 | Whois信息 |

|  |  |
| --- | --- |
| 编号 | 9 |
| 名称 | 获取样本检测结果（result）Get\_result |
| 输入 | 样本ID |
| 输出 | 检测结果 |

|  |  |
| --- | --- |
| 编号 | 10 |
| 名称 | 获取样本静态信息（文件识别）(sample)Get\_Sample |
| 输入 | 样本ID |
| 输出 | 文件大小、MD5、sha1等静态信息 |

|  |  |
| --- | --- |
| 编号 | 11 |
| 名称 | 获取样本PE节信息(PE\_section)Get\_section |
| 输入 | 样本ID |
| 输出 | 样本PE节信息 |

|  |  |
| --- | --- |
| 编号 | 12 |
| 名称 | 获取样本导入表(pe\_import)Get\_import |
| 输入 | 样本ID |
| 输出 | 导入表信息 |

|  |  |
| --- | --- |
| 编号 | 13 |
| 名称 | 获取样本文件操作目录(file)Get\_file |
| 输入 | 样本ID |
| 输出 | 文件目录 |

|  |  |
| --- | --- |
| 编号 | 14 |
| 名称 | 获取样本注册表操作目录(registry)Get\_registry |
| 输入 | 样本ID |
| 输出 | 注册表目录 |

|  |  |
| --- | --- |
| 编号 | 15 |
| 名称 | 获取样本互斥体操作目录(mutex)Get\_mutex |
| 输入 | 样本ID |
| 输出 | 互斥体目录 |

|  |  |
| --- | --- |
| 编号 | 16 |
| 名称 | 获取与样本相关的域名(sd)Get\_sampleDomain |
| 输入 | 样本ID |
| 输出 | 域名列表 |

|  |  |
| --- | --- |
| 编号 | 17 |
| 名称 | 获取IP威胁情报（IP相关样本）(sd)Get\_ipSample |
| 输入 | IP\_ID |
| 输出 | 样本列表 |

|  |  |
| --- | --- |
| 编号 | 18 |
| 名称 | 获取指向ip的域名（sd,di）Get\_ipDomain |
| 输入 | IP\_ID |
| 输出 | 域名列表 |

|  |  |
| --- | --- |
| 编号 | 19 |
| 名称 | 获取ip的历史域名记录（di）Get\_ipDomainRecord |
| 输入 | IP\_ID |
| 输出 | 记录 |

|  |  |
| --- | --- |
| 编号 | 20 |
| 名称 | 获取搜索ID Get\_searchID |
| 输入 | Ip、域名（整理过的，如去除http等可能的冗余信息）、文件hash（MD5，sha1,sha256） |
| 输出 | id |

|  |  |
| --- | --- |
| 编号 |  |
| 名称 |  |
| 输入 |  |
| 输出 |  |

|  |  |
| --- | --- |
| 编号 |  |
| 名称 |  |
| 输入 |  |
| 输出 |  |

|  |  |
| --- | --- |
| 编号 |  |
| 名称 |  |
| 输入 |  |
| 输出 |  |

|  |  |
| --- | --- |
| 编号 |  |
| 名称 |  |
| 输入 |  |
| 输出 |  |

|  |  |
| --- | --- |
| 编号 |  |
| 名称 |  |
| 输入 |  |
| 输出 |  |

|  |  |
| --- | --- |
| 编号 |  |
| 名称 |  |
| 输入 |  |
| 输出 |  |

|  |  |
| --- | --- |
| 编号 |  |
| 名称 |  |
| 输入 |  |
| 输出 |  |