# 通用接口说明

## 1.1 接口认证

接口采用统一的权限校验，一共两层校验：

* ip白名单：请求api的服务器必须添加到白名单。
* token校验：通过我们提供给用户的appid和key以及时间戳timestamp生成，算法为 appid:key:timestamp通过冒号组合的字符串，然后通过md5加密生成token。后台会对timestamp做校验，十分钟内的请求处理，超过十分钟不处理。Key序列码由一所提供，提供的接口appid统一设置为t\_company\_authcode表查询获取的。

对外提供的每个api的请求都需要三个参数，分别是appid、token、timestamp。

## 1.2返回数据格式

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 变量名 | 字段名 | 必填 | 类型 | 描述 |
| status | 返回状态 | 是 | bool | true表示请求成功，false表示请求失败。 |
| error\_code | 错误代码 | 否 | int | status为false时返回的错误代码 |
| error\_msg | 错误信息 | 否 | string | status为false时返回的错误信息 |
| data | 返回数据 | 否 | List | status为true返回，data里是具体的数据。 |

正确返回：{"status": true, "data": []}

错误返回：{"status": false, "error\_code": 500, "error\_msg": "inner server error"}

# 具体接口说明

## 接口1：获取ip情报数据接口

### 接口说明

Token中的appid约定为sinopec 。

### 接口请求

接口路径: /threatenIntrlligence/getIpList

请求类型： POST

请求参数：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 变量名 | 字段名 | 必填 | 类型 | 示例值 | 描述 |
| appid | appid | 是 | string | "sinopec" | 约定的appid |
| token | Token | 是 | string | "080b1766cacb9fdc32252084337ef609" | 通过冒号组合的字符串，然后通过md5加密生成token |
| timestamp | 时间戳 | 是 | Long | 1577407946 | 当前时间的时间戳 |

curl -X POST '<https://k01.weishi110.cn>:9994/threatenIntelligence/getIpList?appid=[appid]&token=[token]&timestamp=[timestamp]'

### 返回结果

格式：JSON

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段名 | 类型 | 示例值 | 描述 |
| status | 状态 | Bool | true | true表示请求成功，false表示请求失败。 |
| err\_code | 错误代码 | int | 500 | status为false时返回的错误代码 |
| err\_msg | 错误信息 | string | 系统内部错误 | status为false时返回的错误信息 |
| data | 返回数据 | List |  | 查询到情报IP的明细信息 |

data详细信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段名 | 类型 | 示例值 | 描述 |
| Status | 入库操作 | string | + | 更新操作：（+，-，=） |
| ip | IP地址 | string | 8.8.8.8 | ip字符串 |
| Industry | 攻击行业列表 | string | 联通 | 攻击行业列表信息 |
| country | 国家 | string | 中国 | 国家名称 |
| province | 省份 | string | 山东 | 省份名称 |
| city | 城市 | string | 青岛 | 城市名称 |
| type | 类型 | string | 僵尸网络 | 类型 |
| score | 威胁评分 | string | 80 | 70-低危，80-中危，90-高危 |
| StartTime | 攻击起始时间 | datetime | 2020-03-29 22:12:53 | 攻击起始时间 |
| endTime | 攻击结束时间 | datetime | 2020-04-01 09:31:46 | 攻击结束时间 |
| Total | 攻击次数 | int | 123 | 攻击次数 |

返回示例

* 正确返回：

{

    "status": true,

    "data": [

        {

            "status": "+",

            "ip": "047.098.145.110",

            "industry": "商业贸易",

            "country": "中国",

            "province": "浙江",

            "city": "杭州",

            "type": "恶意IP",

            "score": "80",

            "total": 14,

            "endTime": "2020-04-01 09:31:46",

            "startTime": "2020-03-29 22:12:53"

        },…

    ],

    "error\_code": null,

    "error\_msg": null

}

* 错误返回：

{"status": false, "error\_code": 500, "error\_msg": "系统内部错误"}

## 接口2：获取木马情报数据接口

### 接口说明

Token中的appid约定为sinopec 。

### 接口请求

接口路径: /threatenIntelligence/getTrojanList

请求类型： POST

请求参数：

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 变量名 | 字段名 | 必填 | 类型 | 示例值 | 描述 |
| appid | appid | 是 | string | "sinopec" | 约定的appid |
| token | Token | 是 | string | 080b1766cacb9fdc32252084337ef609 | 通过冒号组合的字符串，然后通过md5加密生成token |
| timestamp | 时间戳 | 是 | Long | 1577407946 | 当前时间的时间戳 |

curl -X POST '<https://k01.weishi110.cn>:9994/ threatenIntelligence/getTrojanList?appid=[appid]&token=[token]&timestamp=[timestamp]'

### 返回结果

格式：JSON

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段名 | 类型 | 示例值 | 描述 |
| status | 状态 | bool | true | true表示请求成功，false表示请求失败。 |
| err\_code | 错误代码 | int | 500 | status为false时返回的错误代码 |
| err\_msg | 错误信息 | string | 系统内部错误 | status为false时返回的错误信息 |
| data | 返回数据 | array | [] | 查询到情报木马的明细信息 |

data详细信息

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 字段名 | 字段名 | 类型 | 示例值 | 描述 |
| status | 操作 | string | + | 更新操作：（+，=） |
| fileHash | 文件Hash | string | 420df37… | fileHash 值 |
| fileType | 文件类型 | string | Php，asp | 文件的格式类型 |
| eventType | 发现方式 | string | 1 | 1:subject.webPagePhysicalPath(web访问：http访问),  2:object.file(主机防御：上传/创建),  3:subject.webPagePhysicalPath+object.file,  4:均为空 |
| ips | 攻击IP个数 | Int | 3 | 攻击IP个数 |
| domains | 被攻击域名个数 | int | 14 | 被攻击域名个数 |
| hosts | 主机发现次数 | int | 12 | 主机发现次数 |
| startTime | 第一次发现时间 | datetime | 2020-03-29 22:12:53 | 第一次发现时间 |
| endTime | 最后一次发现时间 | datetime | 2020-04-01 09:31:46 | 最后一次发现时间 |

返回示例

* 正确返回：

{

    "status": true,

    "data": [

        {

            "status": "+",

            "fileHash": "e2c7adb07c88164761bc15f3e2dc7fd050face99aab1b5e3f1bfbee5e3148",

            "fileType": "php",

            "eventType": "2",

            "ips": 0,

            "domains": 0,

            "endTime": "2018-11-07 19:37:06",

            "startTime": "2018-11-07 19:37:06",

            "hosts": 1

        },…

    ],

    "error\_code": null,

    "error\_msg": null

}

* 错误返回：

{"status": false, "error\_code": 500, "error\_msg": "系统内部错误"}