奇安信
新 一 代 网 络 安 全

奇安信 威胁情报系统 TIP 2.0

API 使用手册

修订记录

版本	操作	修订理由及内容摘要	修订人	修订日期
1.0	C	创建	白敏	2018-09-17
1.0	M	修改状态码为表格	李朋举	2018-11-29
1.0	M	添加返回错误状态码说明	卫福龙	2018-11-29
1.1	M	新增失陷检测批量查询 api 接口 ignore_top, ignore_url, ignore_port 的说明，批量查询脚本默认 ignore_top=false	万文杰	2018-12-14
1.2	M	1. botnet_info 变为 compromised_info，列表项的属性变为 latest_compromised_time, malware_type, malware_family。 2. is_botnet 变为 is_compromise	苗永超	2019-01-22
1.3	M	1. white_list 改名为 block_impact 2. malicious_info 新增 is_web_attacker 、latest_web_attack_time 解释说明 3. TIP IP 信誉接口返回无 geo_detail 字段，文档中已删除注解和字段返回	万文杰	2019-01-24
1.4	M	1. 安全通告模块：修改安全通告 curl 、python、请求返回结果展示样式 2. IP 信誉模块：在 api 返回结果的 summary 字段中新增 is_white_list 字段，标记查询 IP 是否是 TIP 中用户自定义的白名单 IP 文件信誉、失陷检测模块未改动	万文杰	2019-03-25
1.5	M	更新安全通告接口，安全通告 api 两个接口合并为一个	李亚琼	2019-04-16
1.6	M	新增文档信息、版本变更记录	白敏	2019-04-17
1.6	M	品牌变更，调整文档模板	李亮	2019-05-05

目 录

1 失陷检测批量查询

1.1 /api/v2/compromise/query

==POST== https:// TIP SERVER IP/api/v2/compromise/query

1.2 Query Params

key	type	value
apikey	string	Your API Key 由威胁情报平台注册生成
param	string	需要查询的 IP、域名、URL。涉及到 URL 查询，如：yzsrdfp.f3322.net,47.100.10.70 多个参数以逗号分隔
ignore_url	bool	是否忽略 IOC 中的 URL 部分内容，ture 为忽略，false 为不忽略。忽略后会产生更多报警，但精度不足可能存在误警
ignore_port	bool	是否忽略 IOC 中的 port 部分内容，ture 为忽略，false 为不忽略。忽略后会产生更多报警，但精度不足可能存在误警
ignore_top	bool	是否忽略全球域名解析中 TOP1000 的域名，ture 为忽略，false 为不忽略。不忽略 TOP 网站可以防止忽略 URL、Port 后由可能带来的大量误警

1.3 CURL

```
curl -X POST \
https:// TIP SERVER IP/api/v2/compromise/query \
  -H 'Content-Type: application/json' \
  -H 'Postman-Token: bab7a7f7-8927-4025-98c4-e4031875a3e4' \
  -H 'cache-control: no-cache' \
  -d '{"param": "yzsrdfp.f3322.net,github.com,47.100.10.70", "apikey": "Your API Key", "ignore_top": false, "ignore_url": true, "ignore_port": true}'
```

1.4 Python

```
import requests

url = "https:// TIP SERVER IP/api/v2/compromise/query"

payload = "{\"param\": \"yzsrdfp.f3322.net,github.com,47.100.10.70\", \"apikey\": \"Your API Key\", \"ignore_top\": false, \"ignore_url\": true, \"ignore_port\": true}"
headers = {
    'Content-Type': "application/json",
    'cache-control': "no-cache",
    'Postman-Token': "6fba2b06-3c06-40b8-895e-1aebd3912f3c"
   }

response = requests.request("POST", url, data=payload, headers=headers)

print(response.text)
```

1.5 Example response


```
{
    "data": [
        {
                "yzsrdfp.f3322.net": [
                    {
                            "alert_name": "DSL4 Botnet C&C 活动事件",
                            "campaign": "",
                            "confidence": "high",
                            "current_status": "active",
                            "etime": "2017-02-06T22:00:52.000Z",
                            "id": "58beaf702a3317408d408c25",
                            "ioc": [
                                  "yzsrdfp.f3322.net",
                                  "0",
                                  ""
                            ],
```

```
                        "ioc_category": "DOMAIN_PORT",
                        "kill_chain": "c2",
                        "malicious_family": [
                              "DSL4"
                        ],
                        "malicious_type": "僵尸网络",
                        "platform": "Windows",
                        "risk": "medium",
                        "tag": [
                              "",
                              "cc"
                        ],
                        "targeted": false
                  }
            ]
      },
      {
            "github.com": []
      },
      {
            "47.100.10.70": [
                  {
                        "alert_name": "GhOst RAT 远控木马活动事件",
                        "campaign": "",
                        "confidence": "high",
                        "current_status": "unknown",
                        "etime": "2018-05-21T16:41:27.000Z",
                        "id": "5b0286370edec6074ce30054",
                        "ioc": [
                              "47.100.10.70",
                              "8080",
                              ""
                        ],
                        "ioc_category": "IP_PORT",
                        "kill_chain": "c2",
                        "malicious_family": [
                              "GhOst"
                        ],
                        "malicious_type": "远控木马",
                        "platform": "Windows",
                        "risk": "high",
                        "tag": [
```

```
                                    "",
                                    "cc"
                                ],
                                "targeted": false
                            }
                        ]
                    }
    ],
        "from": "360 企业安全",
        "msg": "执行成功!",
        "status": 2000,
        "user_defined": []
}
```


1.6 Error Response

状态码	说明
2000	请求成功
4001	参数格式错误
4002	apikey 错误
4003	资源获取失败
4006	请求头错误
4007	请求参数错误
4010	请添加 param

1.7 结果属性及说明

属性	类型	可选值	说明
id	字符串	n/a	每个 ioc 的唯一标示
alter_name	字符串	n/a	告警名称
etime	时间	n/a	最早发布时间
risk	字符串	critical high medium low	风险等级: critical 严重 high 高 medium 中 low 低
malicious_type	字符串		威胁类型: 远控木马

		远控木马 botnet 窃密木马 网络蠕虫 KNOWN APT 勒索软件 黑市工具 流氓推广 其他事件	botnet 窃密木马 网络蠕虫 KNOWN APT 勒索软件 黑市工具 流氓推广 其他事件
malicious_family	数组	Ircbot Hook007 njRAT anjori GameOver Zegost Lodbak VBKrypt Disfa Wapomi Cryptolocker Bamital Dorkbot Conficker P2PGOZ . . . 等等上百个	恶意家族
kill_chain	字符串	general connect download c2 dataleak	general 混合功能远控端 connect 受控后上报配置信息 download 下载恶意软件组件 c2 命令控制通道 dataleak 连接数据放置功能的服务器
confidence	字符串	high medium low	置信度: high 高 medium 中 low 低
campaign	字符串	n/a	攻击团伙名称
targeted	布尔	FALSE TRUE	是否定向攻击
tag	数组	n/a	参考属性
platform	字符串	generic windows linux	影响平台 单个或多个可选值组合

		andriid ios macos other	
current_status	字符串	active sinkhole inactive unknown	当前状态： active 活跃 sinkhole inactive 静默 unknown 未知
ioc	数组	Indicators of Compromise	value1: ioc value2: port，端口为 0 表示任意 value3: uri

2 文件信誉批量查询

2.1 /api/v2/filereputation/query

==POST== https:// TIP SERVER IP/api/v2/filereputation/query

2.2 Query Params

key	type	value
apikey	string	Your API Key 由威胁情报平台注册生成
param	string	需要查询样本的 MD5 或 SHA1， 0000e9d77961f38c6c47a87b04705181 多个参数以逗号分隔

2.3 CURL

```
curl -X POST \
https:// TIP SERVER IP/api/v2/filereputation/query \
  -H 'Cache-Control: no-cache' \
  -H 'Content-Type: application/json' \
  -H 'Postman-Token: 4c73be69-488a-44b0-b34b-2212f94d0886' \
```

```
  -d '{"apikey": "Your API Key", "param":
"0000e9d77961f38c6c47a87b04705181,000ef322d85a14ad12242c221196719966618ae0"}'
```

2.4 Python

```
import requests

url = "https:// TIP SERVER IP/api/v2/filereputation/query"

payload = "{\"apikey\": \"Your API Key\", \"param\":
\"0000e9d77961f38c6c47a87b04705181,000ef322d85a14ad12242c221196719966618ae0\"}"
headers = {
     'Content-Type': "application/json",
     'Cache-Control': "no-cache",
     'Postman-Token': "5b59afa6-482e-43fe-a12b-f5c130115d0c"
   }

response = requests.request("POST", url, data=payload, headers=headers)

print(response.text)
```

2.5 Example response

```
{
     "status": 2000,
     "msg": "执行成功!",
     "user_defined": [],
     "from": "360 企业安全",
     "data": [
         {
                 "0000e9d77961f38c6c47a87b04705181": {
                       "update_time": "2018-09-17 11:48:07",
                       "sha1": "56ebdf9dbaba2477bdcf81697ec8c2adf964cc8b",
                       "network": {
                             "udp": [],
                             "url": [],
```

```
                        "ip": [],
                        "domain": [],
                        "tcp": [],
                        "dns": []
                    },
                    "campaign": null,
                    "scan_time": "2018-09-13 16:50:36",
                    "filetype": null,
                    "malicious": "TRUE",
                    "filename": [],
                    "targeted": false,
                    "filesize": 2443216,
                    "insert_time": "2018-07-01 18:12:39",
                    "malicious_family": "razy",
                    "first_seen": null,
                    "sha256":
"f7118d805ddef7ffcb4598b3354ec8dd57b56e3c4a73fe8d33505c615ddd0427",
                    "ioc": [],
                    "md5": "0000e9d77961f38c6c47a87b04705181",
                    "malicious_type": "Adware"
                }
            },
            {
                "000ef322d85a14ad12242c221196719966618ae0": {
                    "update_time": "2018-09-14 16:45:13",
                    "sha1": "000ef322d85a14ad12242c221196719966618ae0",
                    "network": {
                        "udp": [],
                        "url": [],
                        "ip": [],
                        "domain": [],
                        "tcp": [],
                        "dns": []
                    },
                    "campaign": null,
                    "scan_time": "2018-09-12 13:36:45",
                    "filetype": null,
                    "malicious": "TRUE",
                    "filename": [
                        "X\\u6708\\u4efdXXX\\u5e97\\u7ec8\\u7aef\\u9500\\u552e
\\u8ddf\\u8fdb\\u8868.lnk",
                        "X 月份 XXX 店终端销售跟进表.lnk"
```

```
                    ],
                      "targeted": false,
                      "filesize": 1824,
                      "insert_time": "2018-09-14 15:44:23",
                      "malicious_family": "a1526a3c",
                      "first_seen": null,
                      "sha256":
"8a39e83d0d77f61f7cf12e51067c0842468916d0e8f3e237343948e10a75362a",
                      "ioc": [],
                      "md5": "7281fff572a8eef8595281a7a2ee9534",
                      "malicious_type": "Trojan"
                }
            }
    ]
}
```


2.6 Error Response

状态码	说明
2000	请求成功
4001	参数格式错误
4002	apikey 错误
4003	资源获取失败
4006	请求头错误
4007	请求参数错误
4010	请添加 param

2.7 结果属性及说明

属性	类型	可选值	说明
md5	字符串	n/a	样本对应的 md5
sha1	字符串	n/a	样本对应的 sha1
sha256	字符串	n/a	样本对应的 sha256

malicious	字符串	"TRUE", "FALSE", "UNKNOWN"	样本判定结果
malicious_type	字符串	Botnet 僵尸网络 Ransomware 勒索软件 Trojan 远控木马/窃密木马 ExploitKit 黑市工具 NetWorm 网络蠕虫 Promotion 流氓推广 Virus 恶意病毒 Adware 广告程序 Other 其他	恶意类型
malicious_family	字符串	not-a-virus allaple Disfa Suspicious:highconfidence Suspicious:phishing Rouge Locky Virut Skeeyah . . .	恶意家族
first_seen	时间	n/a	样本最早发现时间
filesize	数字	n/a	样本大小
filetype	字符串	'Mach-O fat binary executable' 'HTML''Win32 EXE' 'Win32 DLL' 'DOC' 'ELF shared library' 'PDF' 'GZIP' 'ZIP' 'DEX' 'Win64 DLL' 'DOCX' 'FPX' 'JPEG' 'Mach-O executable' 'ELF executable' 'Win64 EXE' 'Mach-O dynamic bound bundle' 'ELF object file'	样本类型

		'RAR' 'AI' 'XLS' 'PNG' 'Mach-O dynamic link library' 'MKV' 'GIF' 'Mach-O object file' 'DOS EXE' 'SWF' 'Mach-O fat dynamic link library' 'EPUB' 'XML' 'TAR' 'SVG' 'XLSX' 'BZ2' 'XLSM' 'JSON' 'Win16 EXE' 'Mach-O fat dynamic bound bundle' 'PPT' 'PPTX' 'OGG' 'RTF' 'Torrent' 'ASF' 'Static library' 'JP2' 'DOCM' 'OPUS' 'PHP' 'DOTX' 'MOBI' 'LNK' 'MP3' 'PS' 'PICT' 'TTF' 'TIFF' 'HDP' 'WAV'	

		'DOTM' 'XLSB' 'ISO' 'sh script' 'BMP' 'WEBM' 'M4V' 'WEBP' 'IDML' 'MP4' 'APNG' 'MOV' 'OTF' 'PPSX' 'Mach-O fat static library' 'php script' 'ODT' 'M2T' 'M4A' 'PLIST' 'perl script' 'MAX' 'FLAC' 'PPTM' 'bash script' 'ODS' 'ICS' 'python script' 'XLAM' 'CHM' 'PFB' '3GP' 'XLTX' 'EPS' 'env script' 'POTX' 'PPSM' 'M2TS' 'Mach-O fat object file' 'Mach-O dynamic link library stub' 'TTC' 'DJVU (multi-page)'	

		'Virtual Device Driver' 'VCard' 'ODP' 'Mach-O fat dynamic link library stub' 'MPEG' 'KEY' 'HEIC' 'AVI' 'XLTM' 'WMF' 'FLV' 'RM' 'OGV' 'PSD' 'ODG' 'ODF' 'RIFF' 'ACR' 'csh script' 'PDB' 'MKA' 'expect script' 'XCF' 'ruby script' 'ICC' 'python3 script' 'perl5 script' 'INDD' 'tclsh script' 'CR2' 'DS2' 'PAGES' 'Release' 'VRD' 'MPG/3'	
filename	字符串	n/a	高级文件信誉字段 样本名称

ioc	列表	n/a	高级文件信誉字段 样本相关已知 cnc
network	数组	TCP,UDP ,DNS,IP ,URL ,DOMAIN	高级文件信誉字段 样本已知网络行为

注：证书中高级文件信誉模块与普通文件信誉模块中文件信誉接口字段返回不同

3 IP 信誉批量查询

3.1 /api/v2/ip/query

==POST== https:// TIP SERVER IP/api/v2/ip/query

3.2 Query Params

key	type	value
apikey	string	Your API Key
param	string	113.200.78.18,113.200.78.10 多个参数以逗号分隔

3.3 CURL

```
curl -X POST \
https:// TIP SERVER IP/api/v2/ip/query \
  -H 'Content-Type: application/json' \
  -d '{"apikey": "Your API Key", "param": "113.200.78.18, 1.194.133.47"}'
```

3.4 Python

```
import requests

url = "https://TIP SERVER IP/api/v2/ip/query"

payload = "{\"apikey\": \"Your API Key\", \"param\": \"113.200.78.18,
1.194.133.47\"}\r\n"
headers = {
     'Content-Type': "application/json",
     'Cache-Control': "no-cache",
     'Postman-Token': "ec7d8c84-4ec8-44e5-9318-2f4934417814"
   }

response = requests.request("POST", url, data=payload, headers=headers)

print(response.text)
```

3.5 Example response


```
{
     "status": 2000,
     "msg": "执行成功!",
     "from": "360 企业安全",
     "data": {
          "113.200.78.18": {
               "normal_info": {
                    "is_proxy": false,
                    "latest_proxy_time": "",
                    "block_impact": "1",
                    "user_type": "境内企业",
                    "proxy_type": "",
                    "latest_domain": "estel.vicp.net",
                    "asn_org": "CHINA UNICOM China169 Backbone",
                    "asn": "AS4837",
                    "latest_domain_time": "2016-07-14",
                    "is_idc": false
```

```
            },
              "compromised_info": [
          {
              "latest_compromised_time": "2018-11-17",
              "malware_family": "Generic Trojan",
              "malware_type": "远控木马"
          }
      ],
              "summary": {
                    "ip": "113.200.78.18",
                    "is_compromised": true,
    "is_white_list": false,
                    "block_impact": "1",
                    "network_type": [],
                    "malicious_label": []
              },
                "malicious_info": {
                    "ddos_confidence": "40%",
    "is_brute_force": false,
    "is_ddos": false,
    "is_ddos_active_or_passive": "active",
    "is_malicious": false,
    "is_scanner": false,
    "is_spam": false,
    "is_web_attacker": false,
    "latest_brute_force_time": "",
    "latest_ddos_time": "2019-01-03",
    "latest_malicious_time": "2019-01-03",
    "latest_scanner_time": "",
    "latest_spam_time": "",
    "latest_web_attack_time": "",
    "scanner_confidence": ""
              },
                "geo": {
                    "latitude": "34.263161",
                    "city": "西安",
                    "province": "陕西",
                    "longitude": "108.948024",
                    "country": "中国"
              }
       },
    "1.194.133.47": {
```

```
        "compromised_info": [
            {
                "latest_compromised_time": "2019-01-02",
                "malware_family": "LDX",
                "malware_type": "僵尸网络"
            }
        ],
        "geo": {
            "city": "开封",
            "country": "中国",
            "latitude": "34.797049",
            "longitude": "114.341447",
            "province": "河南"
        },
        "malicious_info": {
            "ddos_confidence": "40%",
            "is_brute_force": false,
            "is_ddos": false,
            "is_ddos_active_or_passive": "active",
            "is_malicious": false,
            "is_scanner": false,
            "is_spam": false,
            "is_web_attacker": false,
            "latest_brute_force_time": "",
            "latest_ddos_time": "2017-11-21",
            "latest_malicious_time": "2019-01-02",
            "latest_scanner_time": "",
            "latest_spam_time": "2018-02-24",
            "latest_web_attack_time": "",
            "scanner_confidence": ""
        },
        "normal_info": {
            "asn": "AS4134",
            "asn_org": "No.31,Jin-rong Street",
            "block_impact": "1",
            "is_idc": false,
            "is_proxy": false,
            "latest_domain": "",
            "latest_domain_time": "",
            "latest_proxy_time": "",
            "proxy_type": "",
            "user_type": "境内家庭"
```

```
            },
            "summary": {
                "block_impact": "1",
                "ip": "1.194.133.47",
                "is_compromised": true,
                 "is_white_list": false,
                "malicious_label": [],
                "network_type": []
            }
        }
    }
}
```


3.6 Error Response

状态码	说明
2000	请求成功
4001	参数格式错误
4002	apikey 错误
4003	资源获取失败
4006	请求头错误
4007	请求参数错误
4010	请添加 param

3.7 结果属性及说明

一级字段	二级字段	字段说明	字段类型	枚举值
geo		地理位置-常规（提供给普通用户使用）	字典	
	country	国家	字符串	

	province	省份/州	字符串	
	city	城市	字符串	
	longitude	经度坐标	字符串	
	latitude	纬度坐标	字符串	
summary		摘要	字典	
	ip	查询的 ip	字符串	
	block_impact	该数据主要表明该 IP 应该加入白名单的建议等级 该等级主要依据该 IP 过去 7 天平均关联的终端数量来制定 关联终端数量越多（例如:大型企业的一个 IP 可能会对应 5000+的终端） 该 IP 加入白名单的建议等级将越高。	字符串	1,2,3,4,5
	network_type	该值主要是对本 IP 涉及的网络类型进行汇总	列表	IDC:IDC 主机 PROXY:代理主机
	malicious_label	该值主要是对本 IP 涉及的恶意标签进行汇总	列表	DDOS： DDOS（分布式拒绝服务） SCANNER：恶意扫描

				SPAM：垃圾邮件 BRUTE：暴力破解
	is_compromised	该值表明该 IP 是否是僵尸主机	布尔	true/false
	is_white_list	该值表明该 IP 是否是自定义的白名单	布尔	true/false
normal_info		常规属性	字典	
	asn	ASN	字符串	
	asn_org	ASN 所属组织	字符串	
	is_proxy	该值表明该 IP 是否是代理	布尔	true/false
	latest_proxy_time	该值表明该 IP 最后一次代理验证通过时间	字符串	
	proxy_type	该值表明该 IP 代理的类型	字符串	HTTP HTTPS VPN sock SSH shadowsock go-agent TOR freegate
	is_idc	该值表明该 IP 是否属于 IDC	布尔	true/false

	user_type	该值表明该 IP 的用户类型	字符串	境内企业 境内 IDC 境内家庭 境内宽带运营商 专用出口 境外企业 境外 IDC 境外家庭
	block_impact	该数据主要表明该 IP 应该加入白名单的建议等级 该等级主要依据该 IP 过去 7 天平均关联的终端数量来制定 关联终端数量越多（例如:大型企业的一个 IP 可能会对应 5000+的终端） 该 IP 加入白名单的建议等级将越高。	字符串	1,2,3,4,5
	latest_domain	最近一次该 IP 对应的域名 如果发现有多个域名，只取其中一个	字符串	
	latest_domain_time	最近一次该 IP 与 lastest_domain 关联的时间	字符串	
compromised_info		该 IP 关联的 Botnet 信息(多条)	列表	
	latest_compromised_time	表示该 ip 最近一次出现失陷信息的时间	字符串	
	malware_type	表示失陷信息的恶意软件所属应用类型	字符串	

	malware_family	表示失陷信息的恶意软件家族信息	字符串	
malicious_info		恶意行为属性：	字典	
	is_malicious	该值表示该 IP 是否存在恶意行为 结果为所有恶意行为的状态汇总 即只要存在任何一种恶意行为，该值即为 true	布尔	true/false
	latest_malicious_time	该值表示该 IP 执行恶意行为的最新时间 结果为所有恶意行为的最新时间汇总 即取最近一次恶意行为的执行时间	字符串	
	is_ddos	该值表示该 IP 是否有 DDOS 攻击的行为	布尔	true/false
	ddos_confidence	该值表示该 IP 是在执行 DDOS 攻击行为的可信度 40% 表明该 IP 执行 DDOS 攻击的可信度较低 80% 表明该 IP 执行 DDOS 攻击的可信度较高	字符串	40% 80%
	is_ddos_active_or_passive	该值表示该 ip 发起的 ddos 攻击类型是主动的还是被动 目前只有反射放大利用型的攻击被归纳为 passive 攻击	字符串	active/passive
	latest_ddos_time	该值表示该 ip 最近一次发起 DDOS 攻击的时间	字符串	
	is_scanner	该值表示该 IP 是否有恶意扫描的行为	布尔	true/false

	scanner_confidence	该值表示该 IP 是在执行恶意扫描行为的可信度 40% 表明该 IP 执行恶意扫描的可信度较低 80% 表明该 IP 执行恶意扫描的可信度较高	字符串	40% 80%
	latest_scanner_time	表示该 ip 最近一次发起恶意扫描的时间	字符串	
	is_spam	该值表示该 IP 是否有滥发邮件的行为	布尔	true/false
	latest_spam_time	表示该 ip 最近一次滥发邮件的时间	字符串	
	is_brute_force	该值表示该 IP 是否有暴力破解的行为	布尔	true/false
	latest_brute_force_time	表示该 ip 最近一次执行暴力破解的时间	字符串	
	is_web_attacker	该值表示该 ip 是否有 web 攻击的行为	布尔	true/false
	latest_web_attack_time	表示该 ip 最近一次执行 web 攻击的时间	字符串	

4 安全通告查询

4.1 /api/v2/notice/content

==GET== https:// TIP SERVER IP/api/v2/notice/content

4.2 Query Params

可选参数	数据类型	数据样例	查询参数说明
Api-Key	string	Your API Key	Your ApiKey
page_num	string	1	页码

page_size	string	10	每页通告数量
category	中文	威胁分析	通告类型
start_time	timestamp	1489462072	时间区间上限
end_time	timestamp	1552534072	时间区间下限
industries	string	Finance	影响行业
aggressor_type	string	State Sponsored	攻击者类型
author	string	360	通告发布机构
options	string	aggressor_type,industry,category	查询参数可选范围

4.3 CURL

```
curl "https://TIP SERVER IP/api/v2/notice/content?
page_num=1&page_size=6&start_time=1515502667&end_time=1547038667&category=威胁分析
&industries=Finance&aggressor_type=State Sponsored&
options=aggressor_type,industry,category " -H "Api-Key: Your API Key" -k
```

4.4 Python

```
#!/usr/bin/python
# -*- coding: utf-8 -*-
import requests
baseUrl = "https://TIP SERVER IP/api/v2/notice/content "
headers = {'Api-Key':"Your API Key"}
params = {'page_num':'1', 'page_size': '6','start_time':'1515502667',
'end_time':'1547038667', 'category':'威胁分析', 'industries':'Finance',
'aggressor_type': 'State Sponsored', 'options':'aggressor_type,industry,category'}
response = requests.get(baseUrl, params=params, headers=headers, verify=False)
print(response.text)
```

4.5 Example response

```
{
    "msg": "\u6267\u884c\u6210\u529f!",
```

```
    "industry":[
            "Aerospace",
            "Agriculture",
            "Chemical",
            "Construction",
            "Defense",
            "Education",
            "Energy",
            "Finance",
            "Government",
            "Healthcare",
            "Hospitality",
            "Manufacturing",
            "Media",
            "NGO",
            "Retail",
            "Semiconductor",
            "Technology",
            "Telecommunications",
            "Transportation",
            "nonspecific"
    ],
      "industry_cn":[
            "航空业",
            "农业",
            "化学工业",
            "建筑业",
            "防务",
            "教育业",
            "能源行业",
            "金融行业",
            "政府",
            "健保行业",
            "医疗行业",
            "制造业",
            "媒体行业",
            "非政府组织",
            "零售行业",
            "半导体行业",
            "科技行业",
            "通讯行业",
            "运输行业",
```

```
            "非特定行业"
    ],
      "category_cn": [
            "漏洞通告",
            "安全事件",
            "威胁分析",
            "其它"
    ],
    "aggressor_type": [
            "Organized Crime",
            "Hacktivist",
            "State Sponsored",
            "Insider",
            "Other"
    ],
      "aggressor_type_cn": [
            "网络犯罪组织",
            "黑客行为主义者",
            "国家背景组织",
            "内部人员",
            "其它"
    ],

      "notices": [
    {
                  "abstract": "2018 年 10 月 9 日，US-CERT 发布了一个安全通告***360 威胁情报中心发此通告提醒用户和企业尽快采取必要防御措施以保证网络的可用性。",
                  "aggressor_type": "State Sponsored",
                  "aggressor_type_cn":"国家背景组织",
                  "area": ["中国",
                        "美国",
                        "爱尔兰",
                        "南美"],
                  "author": "360 威胁情报中心",
                  "campaign": ["Gorgon"],
                  "category": "漏洞通告",
                  "degree": "High",
                  "degree_cn": "高",
                  "industries": ["nonspecific"],
                  "industries_cn": ["非特定行业"],
                  "ioc_local": "https:// TIP SERVER IP
/notice_data/aa3cf3158d3514a7e05db67eb8cfdcdf.json",
```

```
                "publish_time": "2018-10-12 19:17:50",
                "related_link": [
                    {
                            "pdf_link": "https://TIP SERVER
IP/notice_data/aa3cf3158d3514a7e05db67eb8cfdcdf.pdf",
                            "source_link": "https:// TIP SERVER
IP/notice_data/html/5bc082c3b3601b003b0bcba1.html"
                    }
            ],
              "tag": [
                    "CVE-2018-17919",
                    "XIONGMAI",
                    "硬编码",
                    "内置账号"
            ],
              "title": "360TI-SV-2018-012 XMeye P2P 云服务器内置硬编码账号漏洞通
告"
        },
          Object{...}
   ],
     "num_total": 15,
     "status": "2000"
}
```


4.6 Error Response

状态码	说明
2000	请求成功
4001	参数格式错误
4002	apikey 错误
4003	资源获取失败
4006	请求头错误
4007	请求参数错误
4010	请添加 param

4.7 结果属性及说明

1、通告内容字段说明：

字段名	含义	数据样例	格式
abstract	摘要	"2018 年 10 月 9 日，US-CERT 发布了一个安全通告***"	字符串
aggressor_type	攻击类型英文	"State Sponsored"	字符串
aggressor_type_cn	攻击类型中文	"国家背景组织"	字符串
area	影响区域	["中国", "美国", "爱尔兰","南美"]	列表
author	发布厂商	"360 威胁情报中心"	字符串
campaign	攻击团伙	["Gorgon", “abc”]	列表
category	通告类型	"漏洞通告"	字符串
degree	威胁等级英文	"High"	字符串
degree_cn	威胁等级中文	"高"	字符串
industries	影响行业英文	["nonspecific"]	列表
industries_cn	影响行业中文	["非特定行业"]	列表
ioc_local	stix 文件完整路径	"https://.***json"	字符串
related_link	相关 url 和 pdf 完整路径组	[{ "pdf_link": "https://.***pdf", "source_link": "https://***.html" }, {...}, {...}]	列表
tag	标签	["CVE-2018-17919", "XIONGMAI", "硬编码", "内置账号"]	列表
title	标题	"360TI-SV-2018-012 XMeye P2P 云服务器内置硬编码账号漏洞通告"	字符串

2、部分查询参数可选列表及翻译字段说明：

注意事项： industry、aggressor_type 需要用英文参数做查询。

字段名	含义	数据样例	格式
industry	摘要	["Aerospace", "Agriculture"***]	列表
industry_cn	行业类型中文	["航空业","农业","化学工业",***]	列表
category_cn	通告类型中文	["漏洞通告","安全事件",**],	列表
aggressor_type	攻击类型	["Organized Crime","Hacktivist",**]	列表
aggressor_type_cn	攻击类型中文	["网络犯罪组织","黑客行为主义者",***]	列表