1. **情报评价**

ioc

ioc类型

恶意评价

最高威胁等级

最高情报可信度

sha1（仅file有值）

sha256（仅file有值）

文件名称(file\_name 仅file有值）

文件大小(file\_size 仅file有值）

文件类型(file\_type 仅file有值）

情报类型

威胁等级

情报可信度

是否有评价标签

情报标签数组

发现时间

更新时间

是否过期

数据源

1. **情报关系检索**

IOC值

IOC类型

对象类型

Value（IOC值，其他存ID）

relation\_type

relation\_order

1. **域名解析**

域名

解析类型

发现时间

解析值

1. **WHOIS信息**

域名

注册域名

注册人

联系邮箱

联系电话

所属组织

国家地区

注册地址

注册时间

到期时间

更新时间

注册商

WHOIS服务器

DNS服务器

域名状态

1. **IP地理位置**

IP

IP类型

国家

省份/州

城市

IP注册机构

AS组织名称

ASN

网络类型

纬度

经度

1. **IP开放端口**

IP

Ip类型

端口

网页标题

网页内容

banner 软件信息版本

1. **攻击组织**

组织唯一ID

组织名称

内部编号（空值）

别名

组织介绍

组织类型

发现时间

最近活跃时间

组织位置

目标行业

目标国家、地区

常用语言

情报来源(爬虫)

攻击方式

1. **恶意家族**

家族唯一ID

家族名称

内部编号（空值）

家族介绍

发现时间

1. **情报资讯**

report主体：

报告唯一ID

标题

作者

报告时间

内容简介

内容

原文链接

情报类型

情报标签

情报来源（电子科大）

来源分类（公众号/技术博客/社交媒体/厂商情报订阅）

攻击行业（[“教育”，”金融”]）

涉及组织

攻击国家/地区

下载链接

共享范围(0 全部)

共享行业（空值）

以及title关联的ioc信息

ioc

ioc类型