奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周

冬奥场景的高对抗威胁情报运营实践

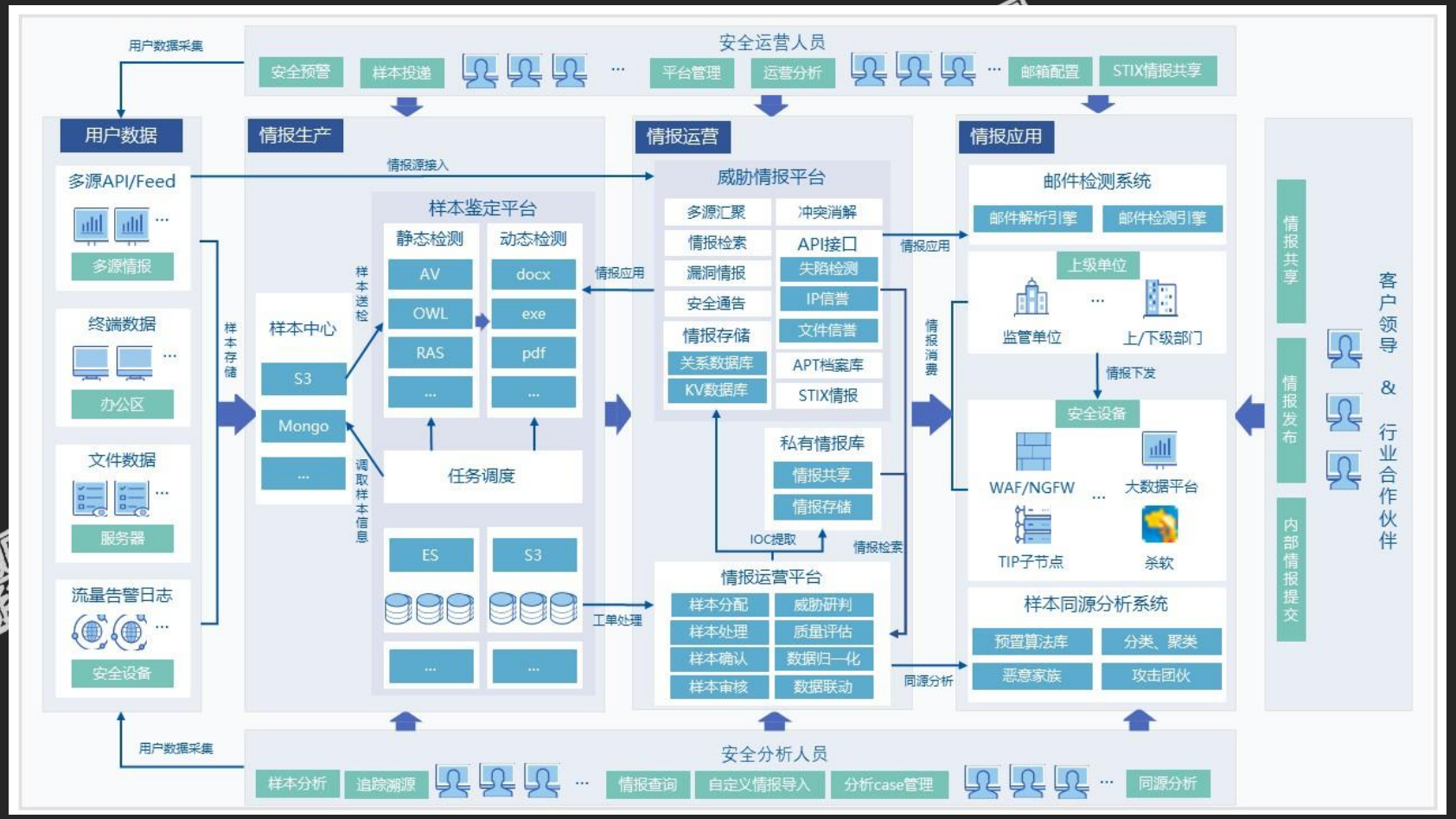
汪列军 奇安信集团威胁情报中心负责人

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

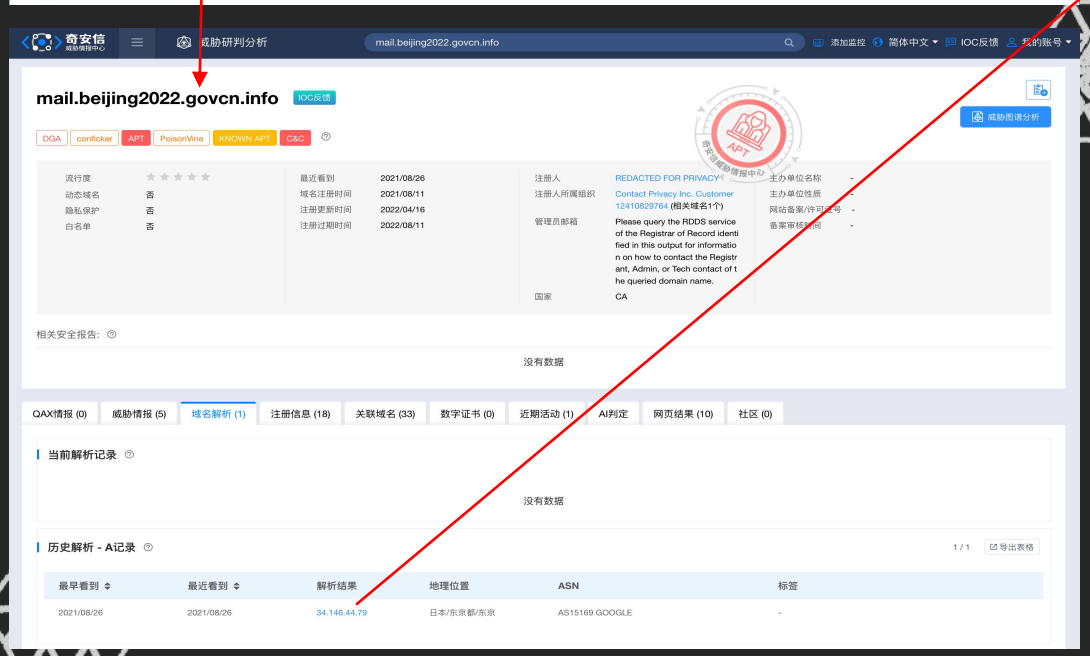
基于本地数据的情报内生系统首次应用

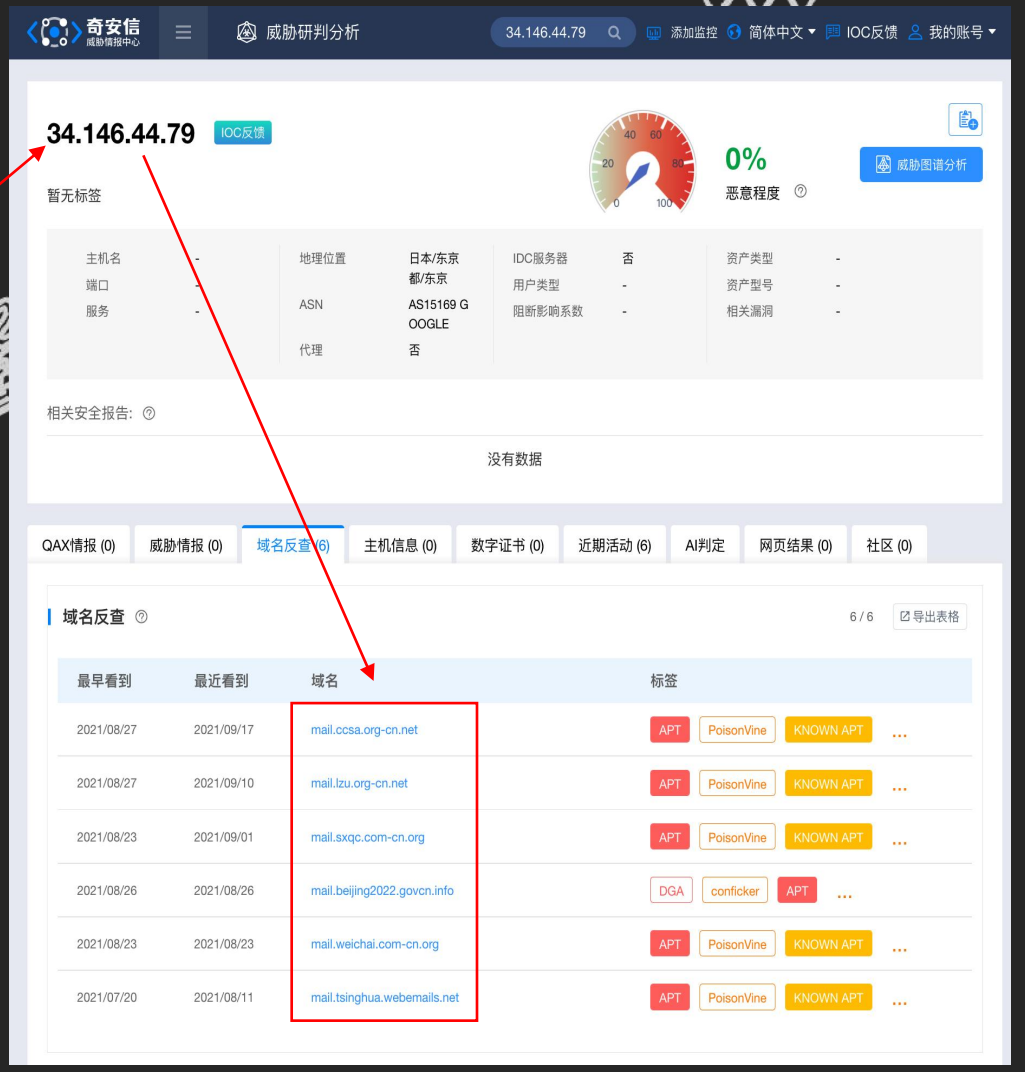
- TIOS本地威胁情报运营平台，以TIP为核心收集过滤融合情报
- 首次公司外的大型活动中部署
- 基于本地的基础数据：文件、网络流量、检测日志
- 利用自有和环境内的检测引擎输出



本地与云端结合的APT活动发现与拓展

https://ti.qianxin.com





本地与云端结合的涉奥攻击发现与分析

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

发件人: admin <admin@51xianqu.net>
发送时间: 2022年2月7日 19:55
收件人: [redacted]
主题: [redacted]：系统升级

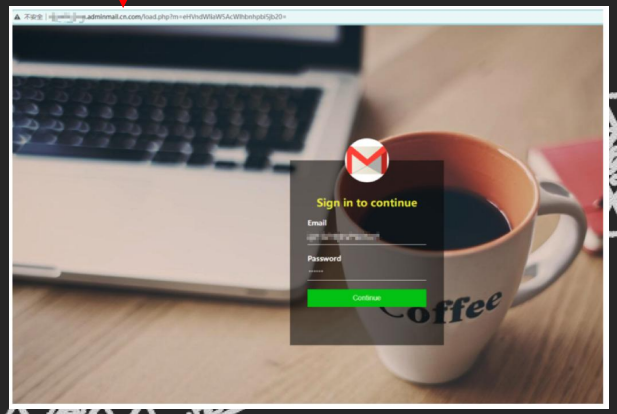
各位同事：

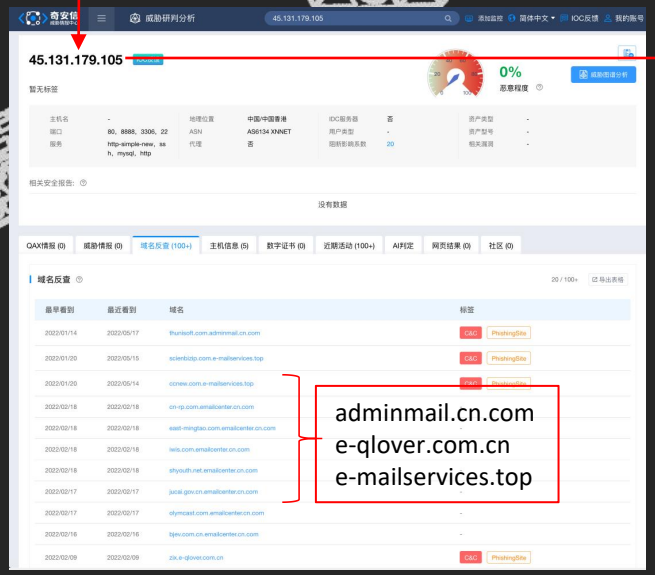
近期由于我公司邮箱密码泄露，服务器IP被限制。公司企业邮箱系统计划于即日起开始进行数据迁移，在此之前，请您务必配合做好以下工作。为保证系统的正常使用。

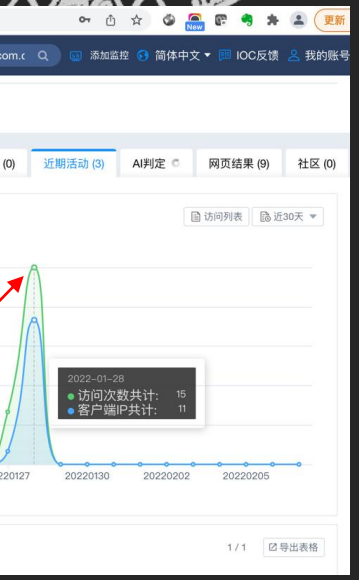
（现需要对邮箱进行升级并需要重新采集用户信息）

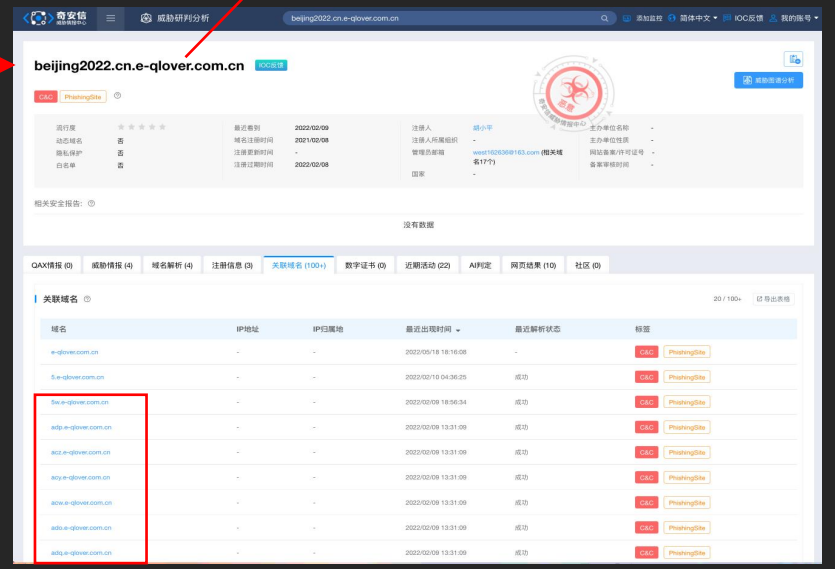
本次升级检测为期7-15天，为此给你带了不便的地方，敬请理解。为保证顺利升级，在接受到结束通知之前，请不要修改账号密码，谢谢配合

点此链接进行升级 → east-mingtao.com.emailcenter.cn.com

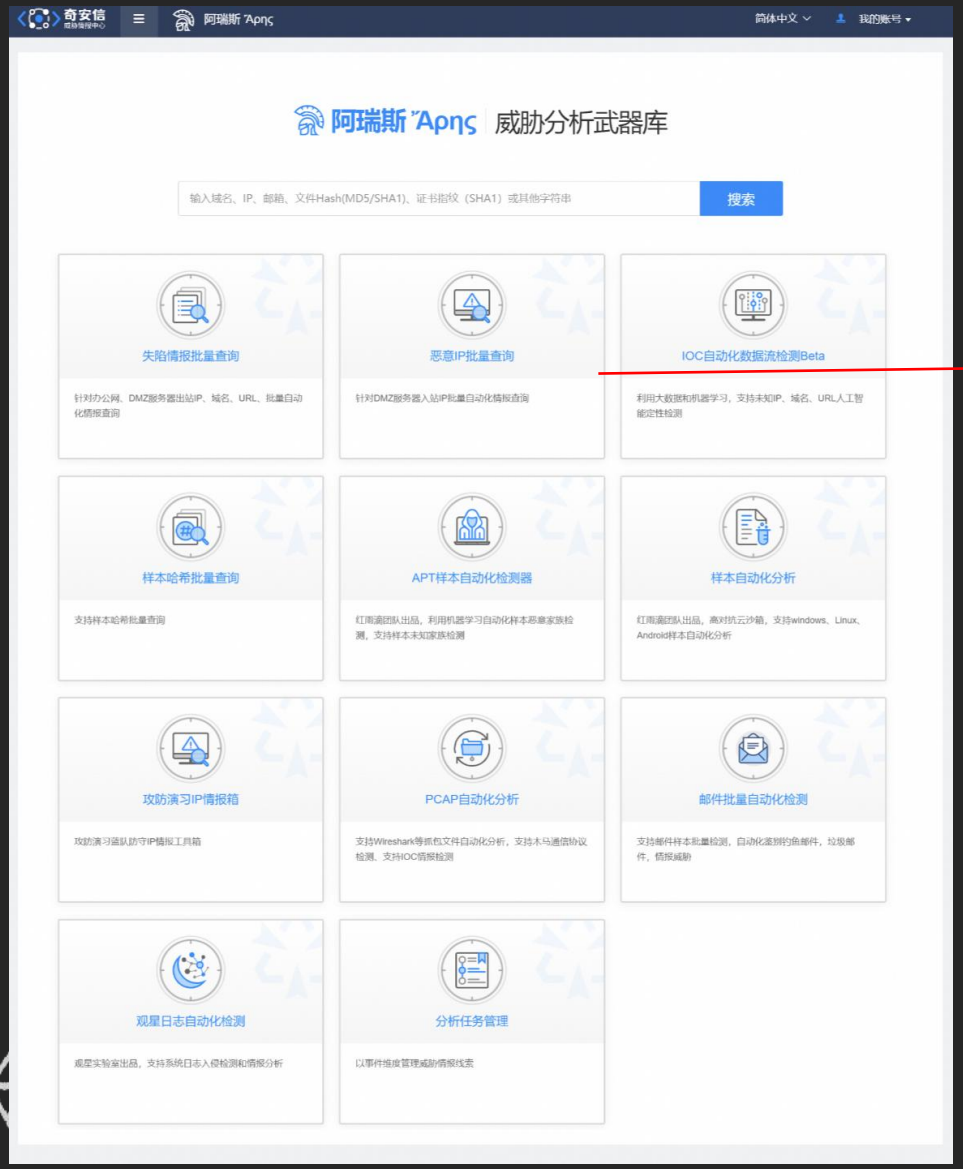








IP等威胁实体的批量研判信息支持



IP	国家	省	城市	经纬度	ASN	运营商	用户类型	是否IDC	是否代理	失陷类型	恶意软件家族	最近失陷时间	否是web atta	web attack	时近发生劫持的时	否是scann	canner置信	近scanner	攻击类型	黑/未命中
203.119.241.34	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-07-09		False				-1
203.119.241.36	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-07-09		False				-1
203.119.241.57	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-05-11		False				-1
203.119.241.58	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1
203.119.241.61	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-05-11		False				-1
59.82.61.97	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2022-01-24		False				-1
106.11.223.175	中国	北京市	北京市	39.902798	AS37963	Hangzhou	Alibaba Ac	False	False				False			False				-1
116.179.32.92	中国	山西省	阳泉市	37.863208	AS4837	CHINA UNI	境内家庭	False	False	bot, bot, b	nymaim, matsnu	2021-04-02, 2021	True	2022-01-28	2022-01-28	False			web_attacker	1
121.46.244.135	中国	上海市	上海市	31.232382	AS4812	China Tel	境内IDC	True	False	远控木马,	Generic Troja	2022-01-24, 2021	True	2022-01-26		False			web_attacker	1
123.125.21.178	中国	北京市	北京市	39.902798	AS4808	China Unicom Beijir		False	False	僵尸网络,	Tofsee, Phish	2020-05-05, 2020	True	2022-01-28	2022-01-19	False	80%	2019-08-2	web_attacker	1
203.119.156.103	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-29		False				-1
203.119.156.123	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-19		False				-1
203.119.156.238	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-19		False				-1
203.119.156.99	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-30	2022-01-05	False				-1
203.119.241.37	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-05-14		False			web_attacker	-1
203.119.241.39	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-03		False				-1
203.119.241.41	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-07-31		False				-1
203.119.241.46	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-07-29		False				-1
203.119.241.47	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-03		False				-1
203.119.241.49	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-09-10		False				-1
203.119.241.54	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-05-14		False				-1
207.46.13.61	美国	华盛顿	昆西	47.234219	AS8075	MICROSOFT	境内IDC	True	False	bot, bot, b	zeus, nymaim,	2020-01-30, 2020	True	2022-01-27	2022-01-11	False	40%	2019-08-0	web_attacker	1
40.77.167.101	美国	弗吉尼亚州	博伊顿	36.665713	AS8075	MICROSOFT	境内IDC	True	False				False	2021-11-09	2022-01-05	False	40%	2019-08-02		-1
47.101.182.7	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False	bot, bot, b	nymaim, tinba,	2021-03-26, 2021	False	2021-09-08	2021-11-10	False				-1
47.101.187.41	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False	bot, bot, b	matsnu, ranbyi	2021-03-07, 2021	False	2021-10-20	2021-11-17	False				-1
47.97.204.168	中国	浙江省	杭州市	30.255611	AS37963	Hangzhou	境内IDC	True	False	bot, bot, b	nymaim, matsnu	2021-03-12, 2021	False	2021-01-12	2021-03-26	False				-1
106.11.223.174	中国	北京市	北京市	39.902798	AS37963	Hangzhou	Alibaba Ac	False	False				False			False				-1
203.119.156.125	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-19	2022-01-28	False				-1
203.119.156.244	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-19	2022-01-19	False				-1
203.119.156.249	中国	上海市	上海市	31.232382	AS37963	Hangzhou	境内IDC	True	False				False	2022-01-20		False				-1
203.119.241.100	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	窃密木马,	IcedID, ELKNO	2022-01-27, 2022	False	2021-12-02	2021-11-09	False				-1
203.119.241.105	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	远控木马,	ChaChi, Cerbe	2022-01-25, 2022	False	2021-11-06	2021-03-30	False				-1
203.119.241.115	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	窃密木马,	Android, Gene	2022-01-27, 2022	False	2021-12-02	2021-01-07	False				-1
203.119.241.122	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	窃密木马,	FormBook, Cob	2022-01-25, 2022	False	2021-12-30	2021-02-12	False				-1
203.119.241.82	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	勒索软件,	Magniber, Adw	2022-01-27, 2022	False	2021-10-29	2021-04-08	False				-1
203.119.241.85	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	黑市工具,	Magnitude, Ma	2022-01-27, 2022	False	2021-11-10	2021-03-10	False				-1
203.119.241.89	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	感染型病毒	Virut, Minerd,	2022-01-25, 2022	False	2022-01-01	2021-04-23	False				-1
203.119.241.93	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False	窃密木马,	EmoDldr, Andr	2022-01-25, 2022	False	2021-11-16	2021-06-26	False				-1
59.82.61.52	中国	北京市	北京市	39.902798	AS37963	Hangzhou	境内IDC	True	False				False	2021-11-23		False				-1
59.82.84.101	中国			39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1
59.82.84.33	中国			39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1
59.82.84.49	中国			39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1
59.82.84.67	中国			39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1
59.82.84.69	中国			39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1
59.82.84.85	中国			39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1
59.82.84.95	中国			39.902798	AS37963	Hangzhou	境内IDC	True	False				False			False				-1

- 云端的SaaS平台为安全分析人员提供了一系列的在线工具
- 对于文件本身的深度检测、批量化的威胁对象查询、PCAP文件和单独导出邮件的解析和基于情报的检测
- IP信息包含多种来源的历史黑活动信息整合，结合IP本身的接入类型可以执行自动化的阻断

奇安信 | BEIJING 2022

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

主动的基于新活动域名分析的威胁狩猎

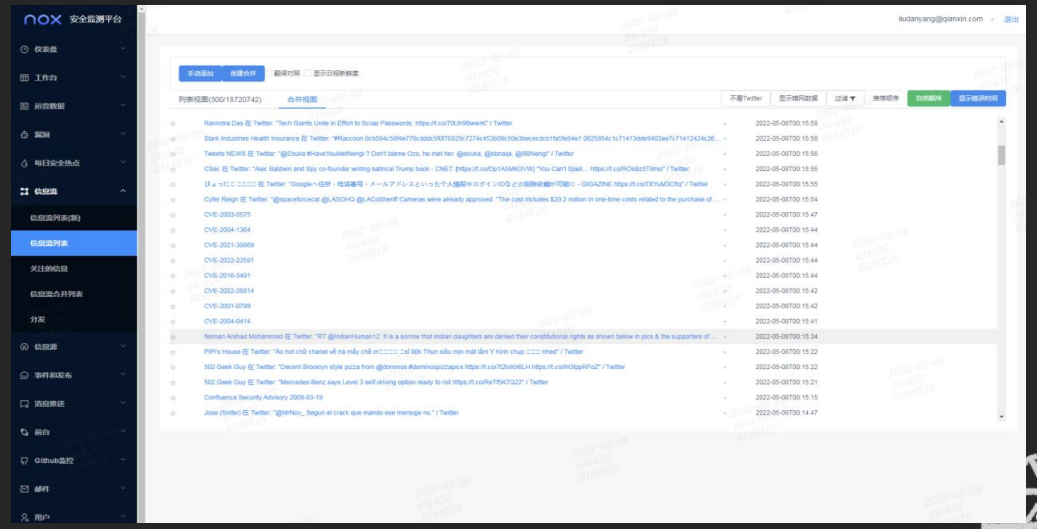
- 基于Passive DNS和Whois数据的主动威胁狩猎
- 通过特征和模型的疑似威胁发现
- 尽可能自动化提高信噪比，最终的人工确认
- 定位线索以后进一步的拓线

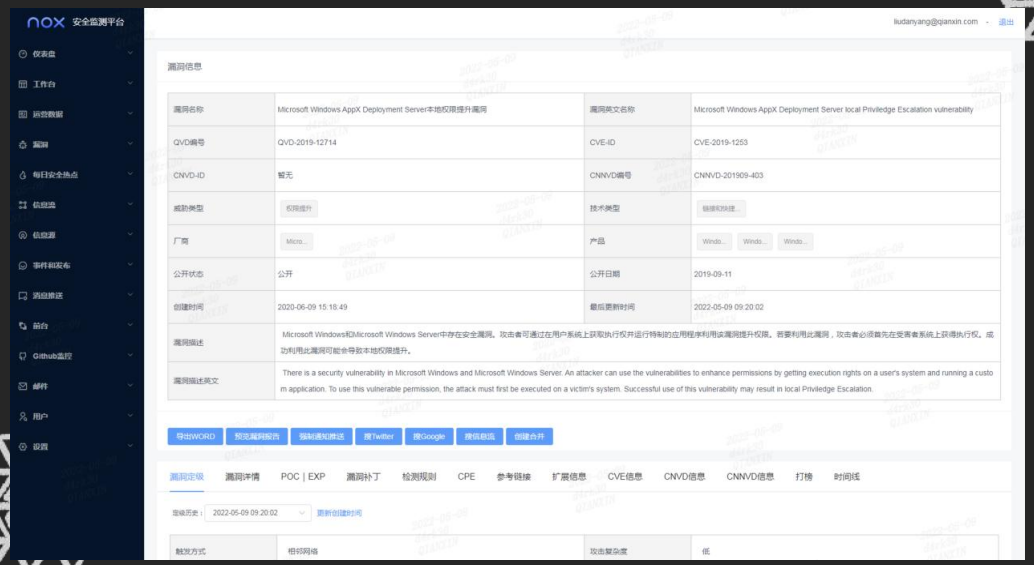
新活动域名	判定结果	说明	研判时间
beijing.keiz-ticket.com	未知	18年前是日本一个售票的平台，20年被重新注册，目前不知	2022/2/1
dongao.bj-2022.com	可疑	直接访问为”冬奥全球传播平台“，建议联系奥组委确认是	2022/2/1
beijing.vipticket.cn	非恶意	[redacted]的域名	2022/2/1
beijing.dongaoacc.com	非恶意	[redacted]培训学校有限公司	2022/2/1
beijing.toupiaoxitong.cn	非恶意	[redacted]网络科技有限公司	2022/2/1
beijing5220224.cn.cnlinfo.net	非恶意	行业信息网，注册的企业的托管在上面的子页面	2022/2/1
beijinghuipiao.com	非恶意	[redacted]汇票，与冬奥无关	2022/2/1
beijinghaoyun.com	黑	某公司主页，被黑下来，挂了色情站点的黑页，但与冬奥无	2022/2/1
beijing52202292.cn.cnlinfo.net	非恶意	行业信息网，注册的企业的托管在上面的子页面	2022/2/1
beijing-olympic.cn	非恶意	08年北京奥运会相关域名	2022/2/1
beijing.mingshipiaowu.top	非恶意	票务相关网站，与冬奥无关	2022/2/1
beijing-2022.key-techno.de	未知	一个blog，主题跟理解奥运会有关系，不是钓鱼	2022/2/1
beijinggupiao.com	黑	某公司主页，被黑下来，挂了色情站点的黑页，但与冬奥无	2022/2/1
beijing.cityofeastbrewtonaltrafficticketattc	非恶意	贸易网站	2022/2/1
olympics2022.net	可疑	疑似博彩站或者钓鱼站点，建议联系奥组委确认是否为官方	2022/2/1
aoyunmenpiao.net	非恶意	[redacted]网，08年注册的，与冬奥无关	2022/2/1
beijing420227.cn.cnlinfo.net	非恶意	行业信息网，注册的企业的托管在上面的子页面	2022/2/1
beijing-olympic-stadium-nordic-style-suit	非恶意	酒店预定网站	2022/2/1
beijing.moretickets.com	非恶意	[redacted]票务	2022/2/1
beijing-2022.xn--6qq986b3xl	可疑	http://beijing-2022.xn--6qq986b3xl/ 可能是仿冒冬奥的	2022/2/1
olympics2022.yunbuzhan.com	未知	非奥组委域名，该网站存在一个子域名（https://xsg.yunbuzhan.com/）为个人博客，博客中描述该系统（奥林匹克云展厅）为毕业设计相关系统，判断应为非恶意域名，加入监测列表。	2022/2/1
beijing52202273.m.cnlinfo.net	非恶意	行业信息网，注册的企业的托管在上面的子页面	2022/2/1
beijing2008menpiao.com	非恶意	08年的网站，与冬奥无关	2022/2/1
beijingfangshanqufapiao.7dbjj3.gov.cn.gf9	非恶意	北京[redacted]票网	2022/2/1
beijing.vipticket.com.cn	非恶意	[redacted]下的域名	2022/2/1
beijingkaizhusushousidingefapiao.qzhuko	非恶意	非奥运相关网站	2022/2/1
beijing.olympic.org	非恶意	1995年注册的域名，访问会跳转到奥委会官网，建议询问是	2022/2/1
beijing.toupiaotp.com	非恶意	投票相关站点，与冬奥无关	2022/2/1
beijing.qichepiao.cn	非恶意	汽车票，与冬奥无关	2022/2/1
beijingqixingpiaoguolvzhuanyingdian.blia	非恶意	旅行社网站	2022/2/1
beijing52202251.m.cnlinfo.net	非恶意	行业信息网，注册的企业的托管在上面的子页面	2022/2/1
beijing.baoyunjiankang.com	非恶意	与冬奥无关	2022/2/1
beijingdiscounttickets.com	非恶意	与冬奥无关	2022/2/1
beijing52202251.cn.cnlinfo.net	非恶意	行业信息网，注册的企业的托管在上面的子页面	2022/2/1

奇安信 | BEIJING 2022

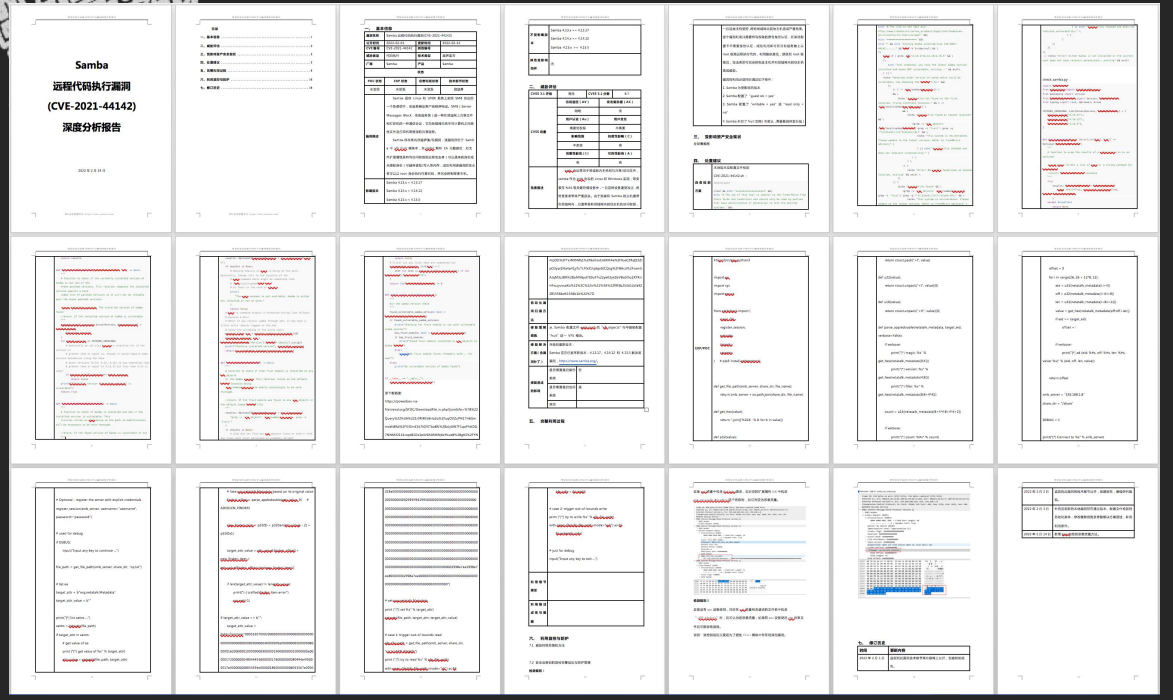
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

冬奥类的大型重要活动的漏洞情报运营





- 业务连续性第一位，基本不可能为了打补丁暂停核心业务系统
- 需要最快速的漏洞应急响应，最全面详细的解决方案
- 强大的运营平台工具、专业的分析人员、高效的经过验证的流程，缺一不可
- 漏洞研判数据漏斗：9500 -> 90 -> 78 -> 17



奇安信 | BEIJING 2022

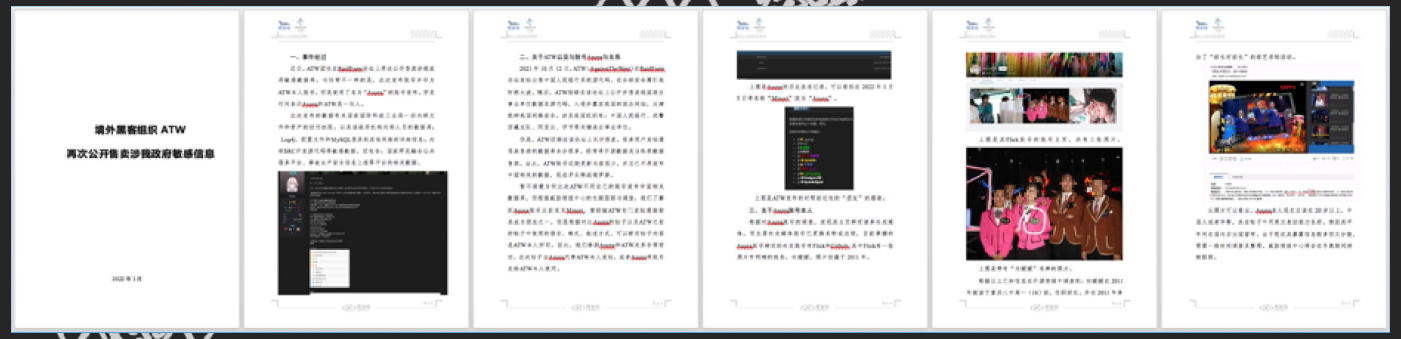
北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

非传统网络攻防层面的威胁情报

52749	32617	4562	2863	1063	1442
社交贴文	账号数	敏感贴文	新闻资讯	报道媒体	敏感新闻

对于所有冬奥相关的多源信息做全面的监控，高热度议题及时发现与介入

对于Internet 2.0公司的高管过往经历挖掘发现非常明显的反华背景



ATW组织相关人员线索的挖掘，发现疑似国内背景的人员


奇安信冬奥网络安全威胁快报

第 13 期　2022 年 2 月 1 日

一、涉网络安全

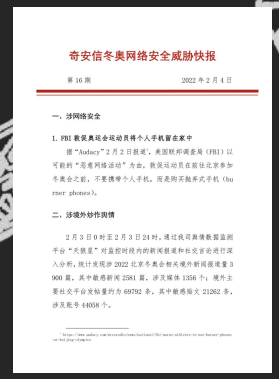
1. 美国联邦调查局（FBI）发布针对冬奥的网络安全警告

北京时间 1 月 31 日，美国联邦调查局警告，威胁行为者可能会针对 2022 年 2 月的北京冬季奥运会和 2022 年 3 月的残奥会，然而，尚未发现此类攻击计划的证据。

“迄今为止，联邦调查局尚未发现任何针对奥运会的特定网络威胁，但鼓励合作伙伴保持警惕，并在其网络和数字环境中保持最佳实践”。

2. 奥运老将因“侵入性监控泄沫”抵制 2022 北京冬奥

北京时间 1 月 31 日，奥运老将、资深观察人士戴维·沃利金斯基（David Wallechinsky）表示，他不会参加 2022 北京冬奥会，因为“中国政府对游客实施了侵入性的‘监视泡沫’”。沃利金斯基还提到《华盛顿邮报》近期声称披露的中国采购文件，该文件显示习近平政府曾撤消各方更标一个软件项目，该软件可以把据“标名西方媒体记者”和其他“政


奇安信冬奥网络安全威胁快报

第 16 期　2022 年 2 月 4 日

一、涉网络安全

1. FBI 称突袭运动员将个人手机留在家中

据“Judacy”2 月 2 日报道，美国联邦调查局（FBI）以可能的“恶意网络活动”为由，敦促运动员在前往北京参加冬奥会之前，不要携带个人手机，而是购买裸机手机（burner phones）。

二、涉境外炒作舆情

2 月 3 日 0 时至 2 月 3 日 24 时，通过我司舆情数据监测平台“天眼星”对监控时段内的新闻报道和社交言论进行深入分析，统计发现涉 2022 北京冬奥会相关境外新闻报道量 3 900 篇，其中境外新闻 2581 篇，涉及媒体 1356 个，境外主要社交平台发帖量约为 69792 条，其中敏感贴文 21262 条，涉及账号 44058 个。

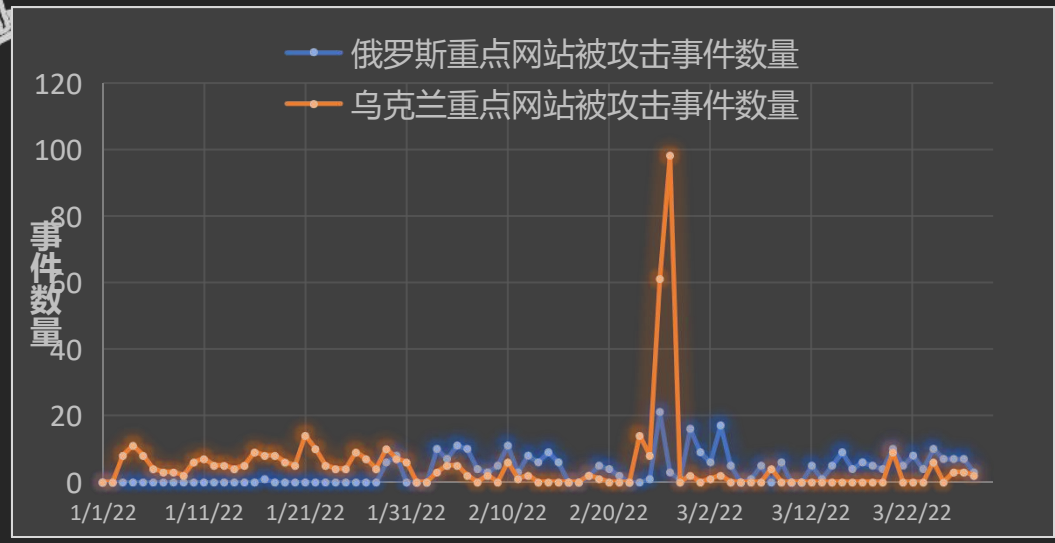

奇安信冬奥网络安全威胁快报

第 18 期　2022 年 2 月 6 日

一、涉网络安全

1. “M72022”获得过多权限引争议 外媒再次建议使用一次性手机

北京时间 2 月 5 日，外媒 Android Central 总结了目前发现的“M72022”个人隐私争议：①该应用程序可完全控制麦克风；②该应用程序将自己强制进入前台，让种安卓用户就不会收到它正在运行的通知；③该应用程序可以随时收集音频；④该应用将音频文件发送到位于中国大陆的服务器；⑤收集的音频由中国人工智能公司科大讯飞处理，该公司因安全问题在美国被列入黑名单；⑥华为、小米、Vivo、魅族和 Oppo 设备的中国品牌手机用户也建议该应用程序将数据发送回制造商。由此，该报道认为外国运动员使用一次性手机的建议非常可靠，该应用程序获得了过多权限。



赛事后期的俄乌冲突，相关的破坏性恶意代码和相互之间的DDoS在网络上掀起的风暴是否对冬奥的形成影响我们需要密切监控

BCS2022系列活动-冬奥网络安全“零事故”宣传周

奇安信

北京2022年冬奥会官方赞助商
Official Sponsor of the Olympic Winter Games Beijing 2022

BCS2022系列活动-冬奥网络安全“零事故”宣传周