2019 西湖论剑·网络安全大会
WEST LAKE CYBERSECURITY CONFERENCE

2018年浙江省互联网网络安全报告

主讲人：ZJCERT 龙泉

CONTENTS
目 录

国家中心情况介绍

国家计算机网络应急技术处理协调中心（以下简称“国家中心”）成立于2002年9月，是中央网络安全和信息化委员会办公室管理领导下的国家级的网络安全应急机构，是我国网络安全应急体系的**核心协调机构**。现已在全国31个省和21个地市成立分中心。

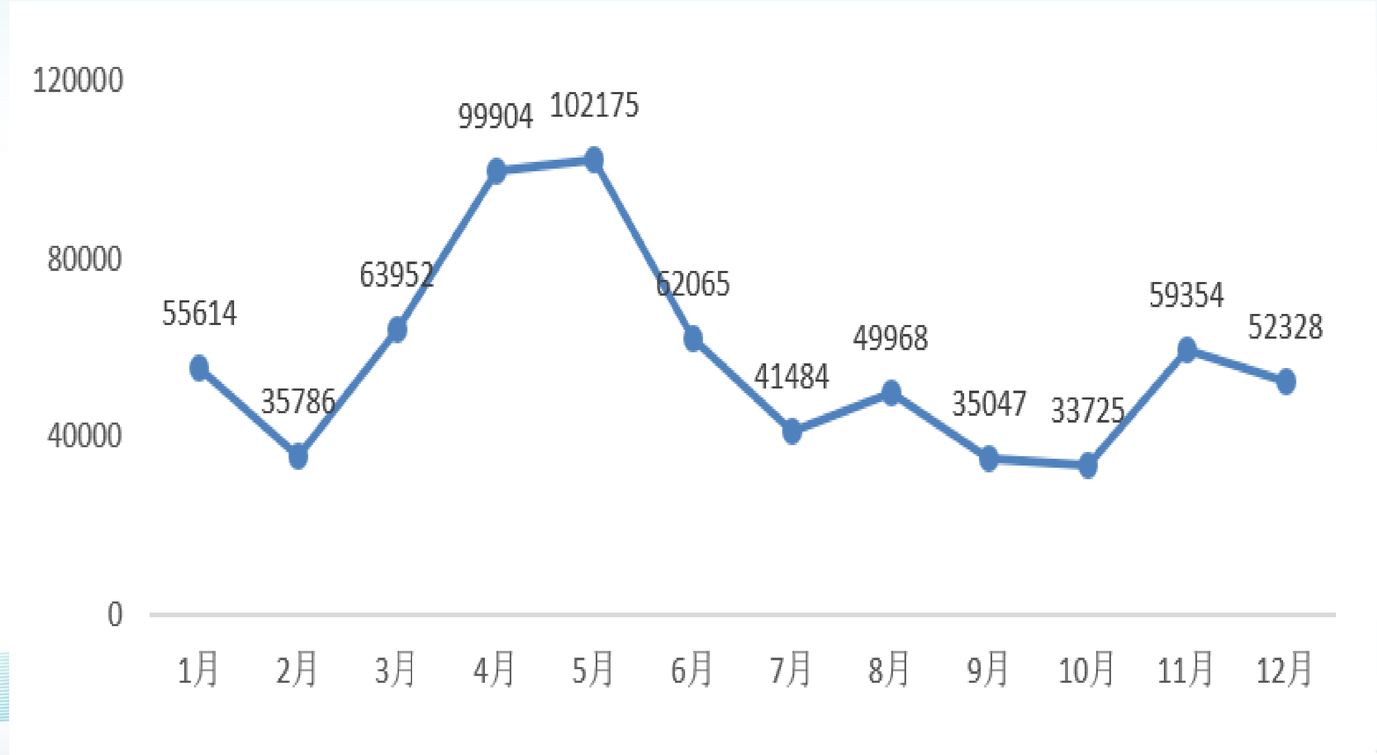
国家中心按照“积极预防、及时发现、快速响应、力保恢复”的方针，积极开展互联网网络安全事件的**预防**、**发现**、**预警**和**协调处置**等工作，维护国家公共互联网安全，保障基础信息网络和重要信息系统的安全运行。

具备的能力优势

- 独一无二的网络安全技术监测平台
- 稳定高效的合作机制
- 政府授权、快速高效处置
- 丰富的网络安全测评经验
- 国内一流的检测实验环境
- 国内顶尖的专业人才队伍

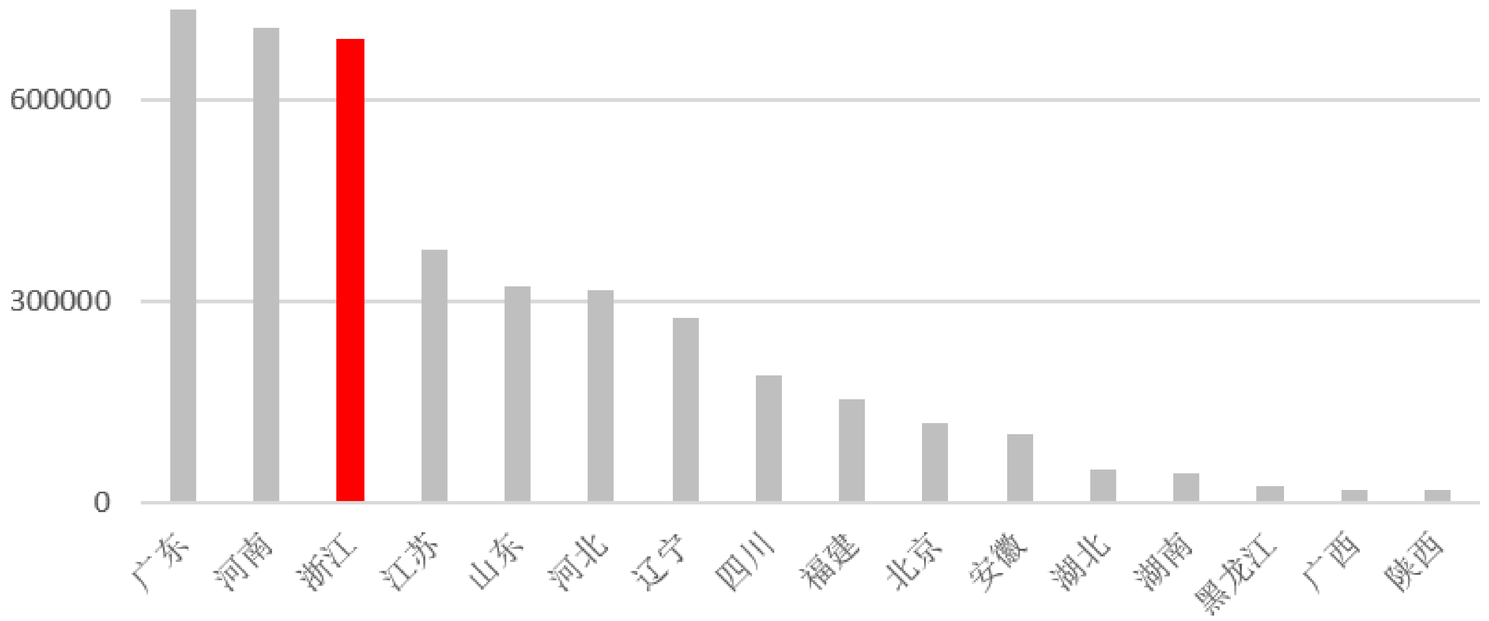
CONTENTS
目 录

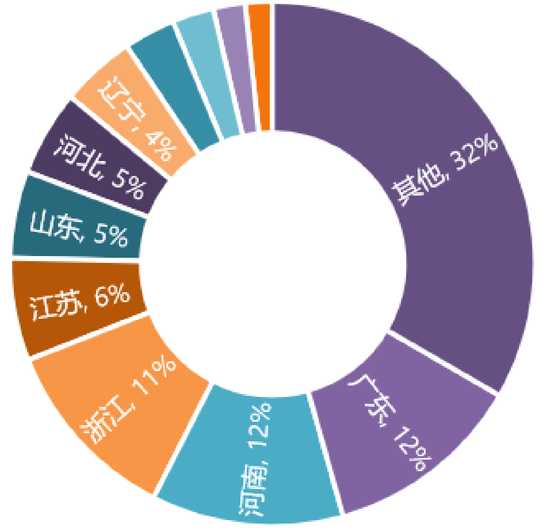
木马或僵尸程序受控主机情况



- 2018年全年浙江省共691,402个IP地址对应的主机被木马或僵尸程序控制；
- 从季度分布情况来看，二季度受控主机数显著多于其他季度，三季度最少；
- 从月度分布情况来看，5月主机感染木马和僵尸数最多，为102,175个，10月份最少，为33,725个。

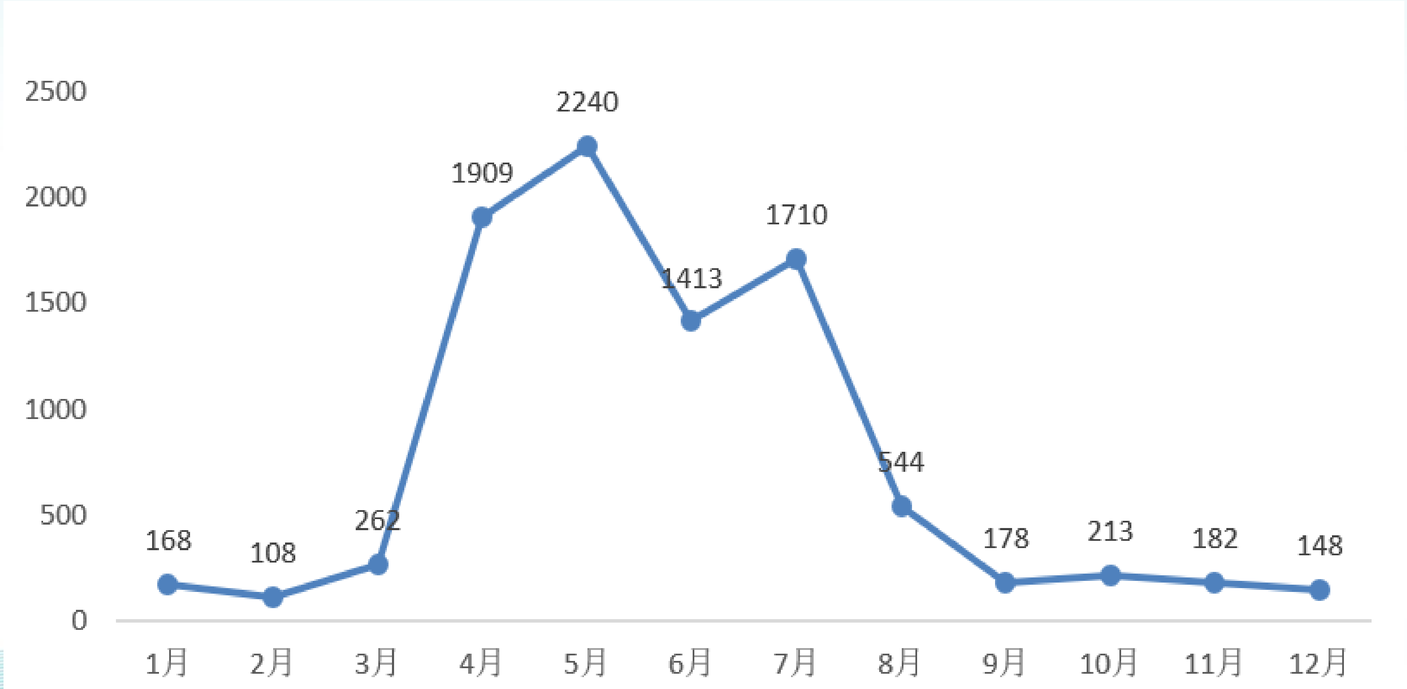
木马或僵尸程序受控主机分析





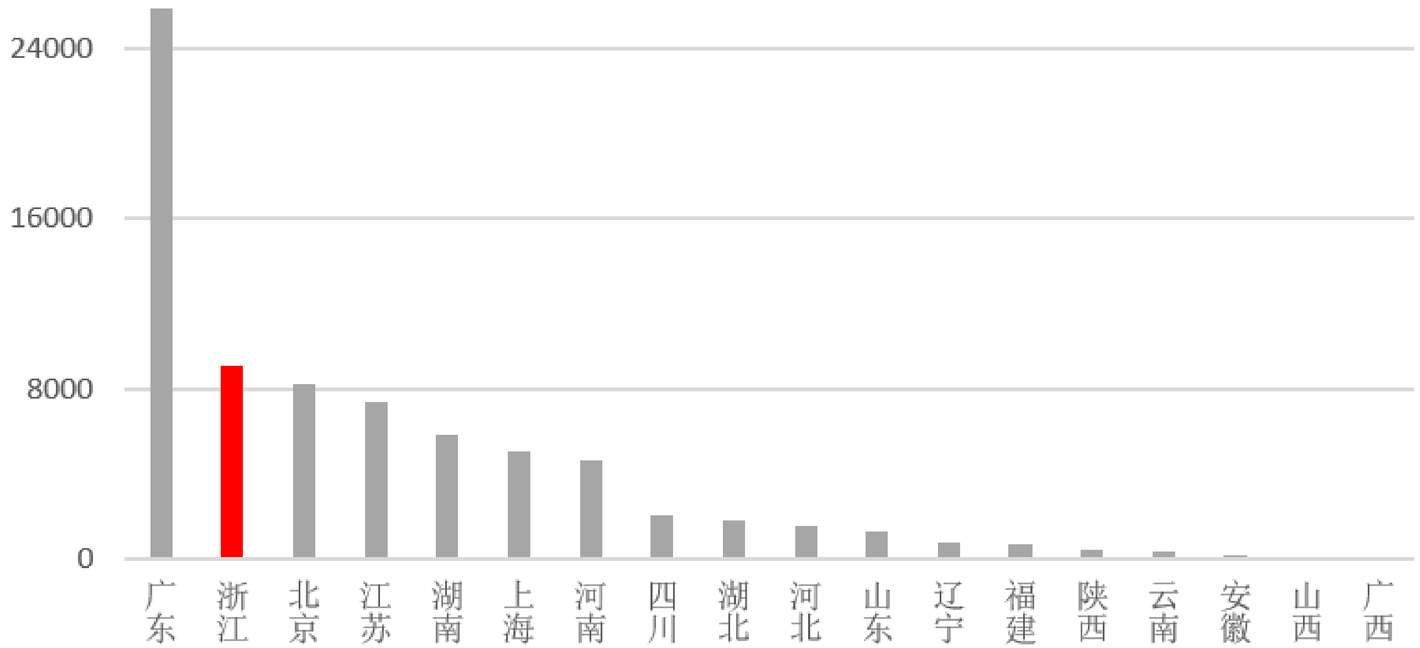
- 2018年**全年境内**共**6,160,473**个IP地址对应的主机被木马或僵尸程序控制；
- 浙江省作为网络较为发达的省份，全年共有**691,402**个IP地址对应的主机被木马或僵尸程序控制，整体数量居全国**第三**；
- 从月度情况看，被木马僵尸控制主机数每月均在**全国前四**。

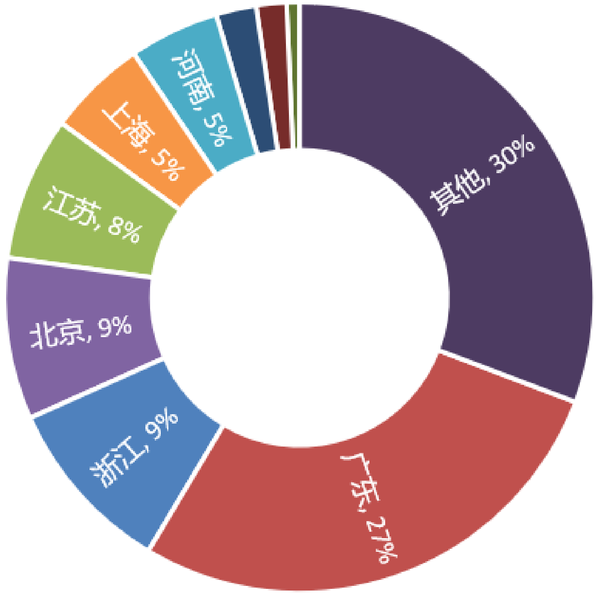
木马或僵尸程序控制主机分析



- 2018年全年浙江省木马或僵尸程序控制服务器有9,075个；
- 二季度增长趋势明显，均值为1,854个；
- 5月份木马或僵尸程序控制服务器最多达到2,240个。

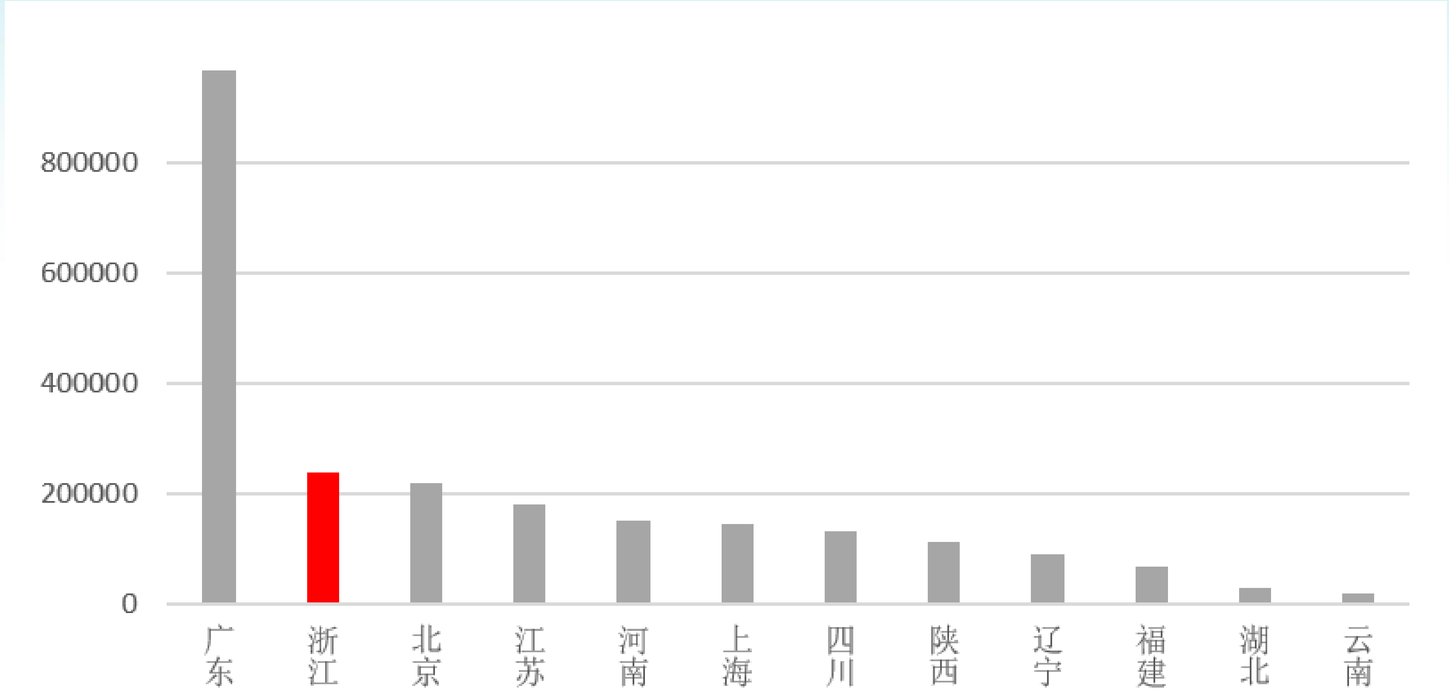
木马或僵尸程序控制主机分析

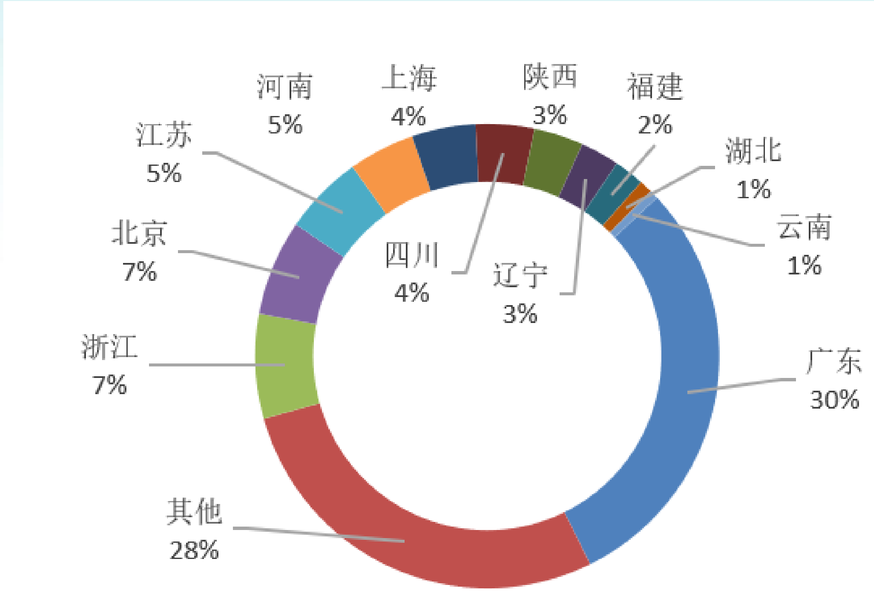




- 2018年**全年境内**木马或僵尸程序控制服务器IP有**96,535**个；
- **浙江省**为**9,075**个，约占全国的**9%**，整体数量占全国数量**第二**；
- **各月**木马僵尸程序控制服务器数在全国**前三到五位**。

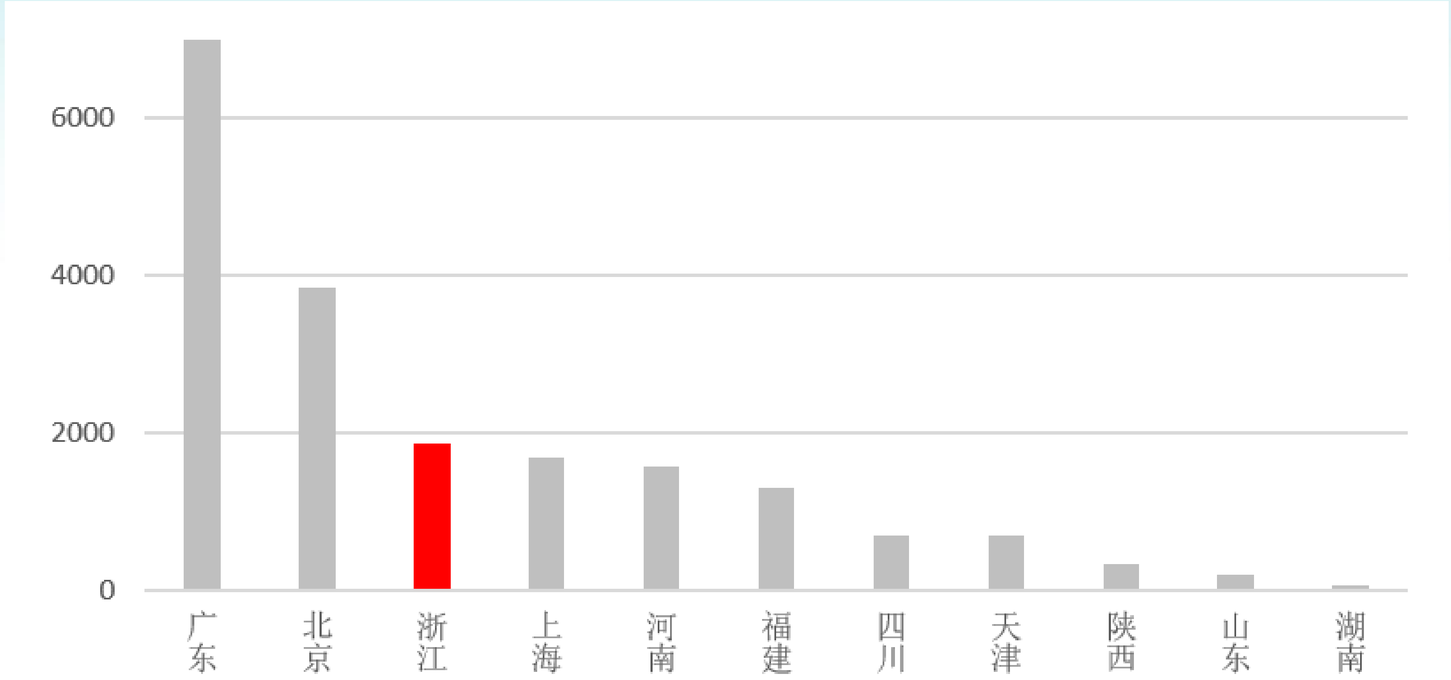
飞客蠕虫事件分析

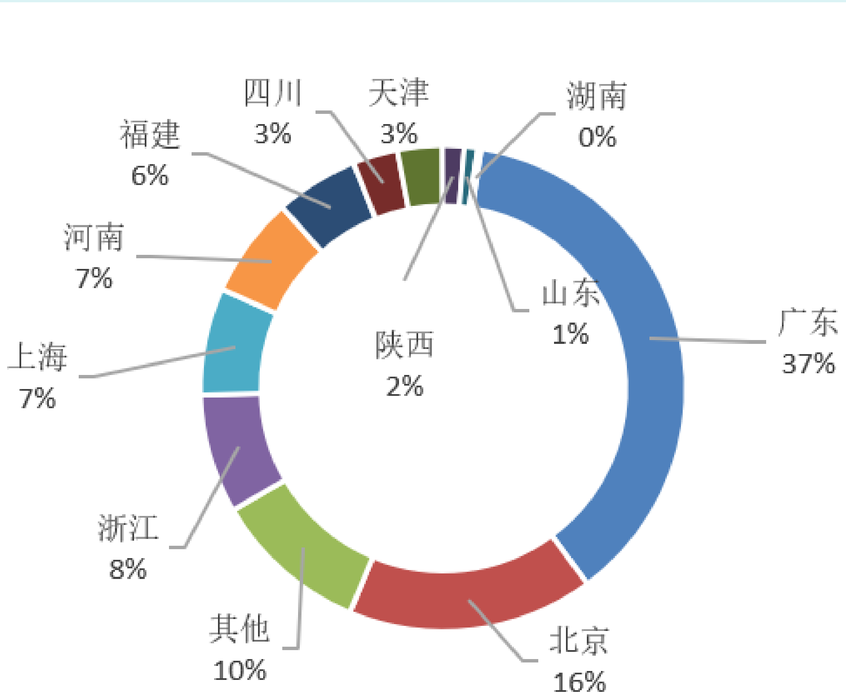




- 2018年全年，境内感染飞客蠕虫的主机IP数为3,265,279个；
- 浙江省238,096个，约占7.3%，仅次于广东省，排名全国第二；

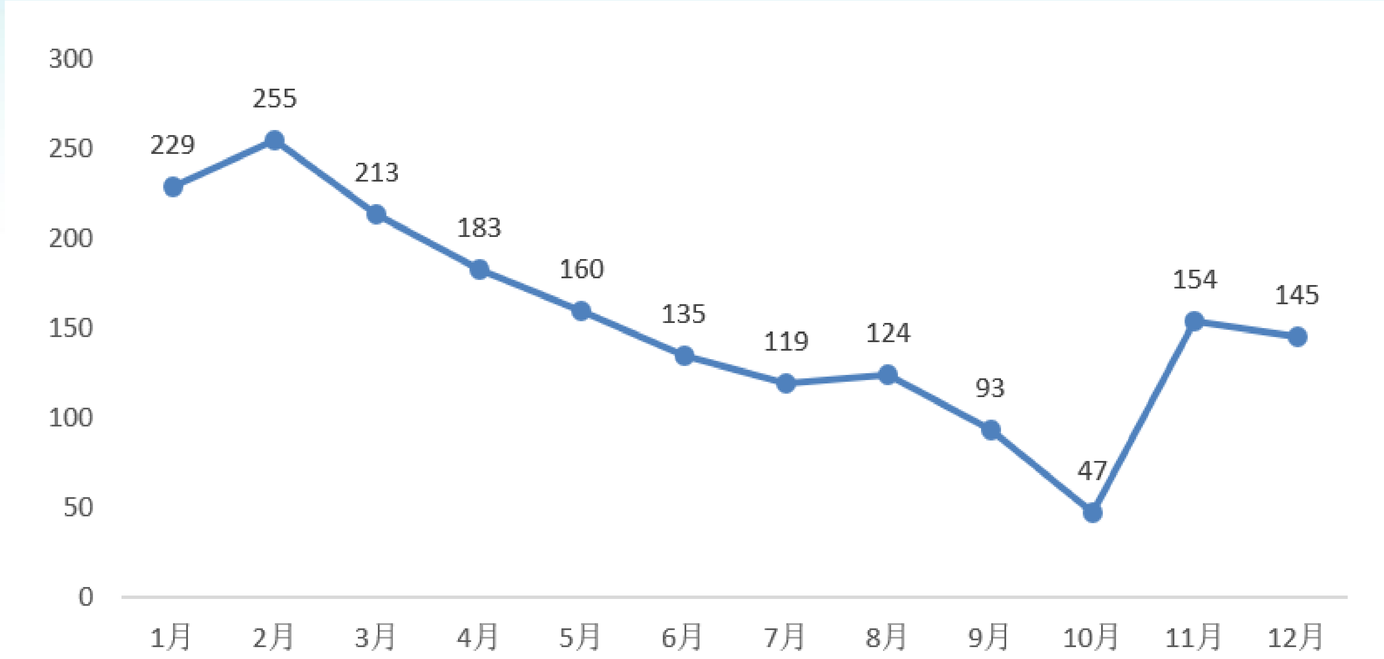
网页篡改数据分析





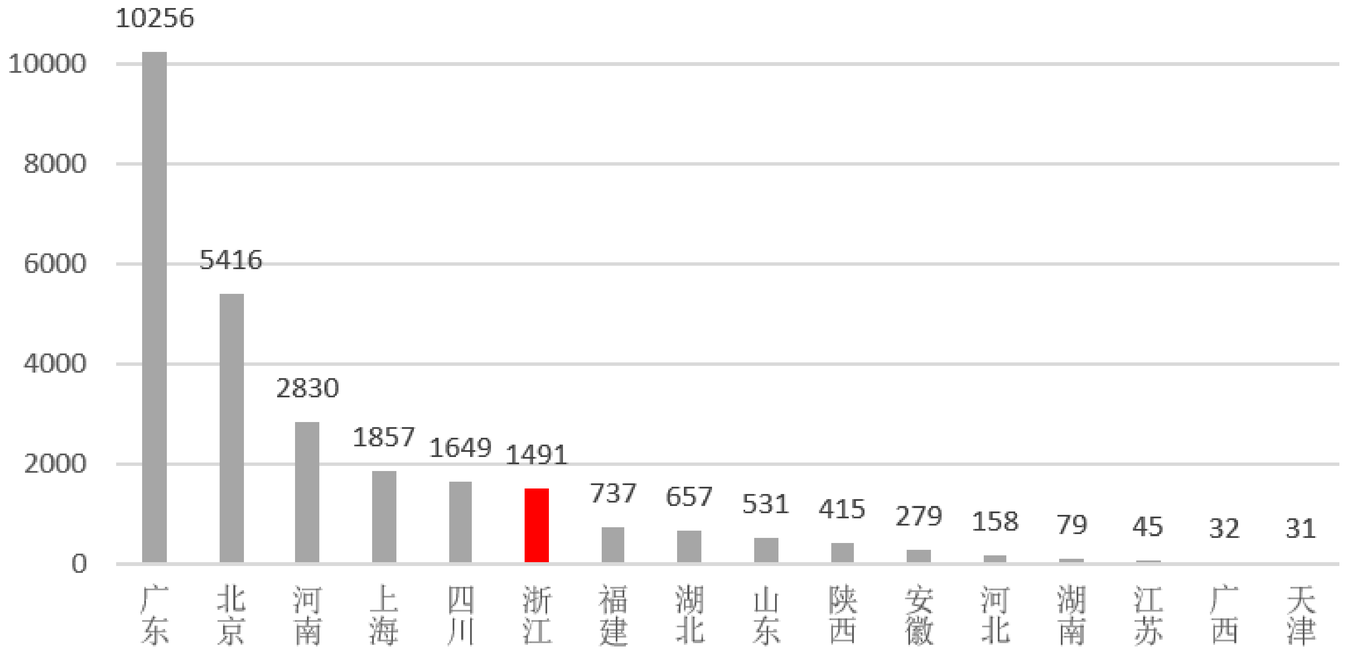
- 2018年**全年**，我国**大陆地区**被篡改网站的数量为**23,459**个；
- **浙江省**被篡改网站数量**1,857**个，约占全国**7.9%**，排名全国**第三**。

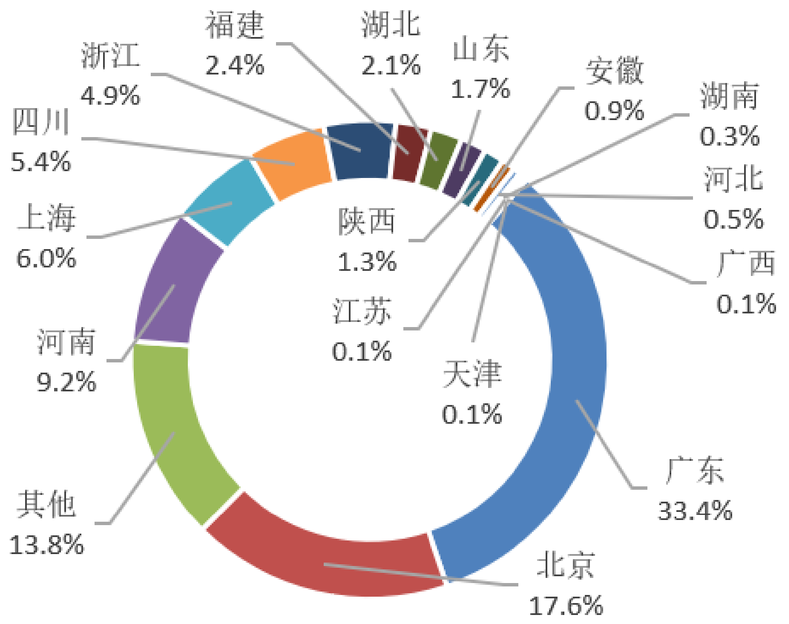
网页篡改数据分析



- 2018年全年，浙江省内被篡改网站数量1,857个；
- 2月被篡改数最多，为255个，10月最少，为47个，总体呈下降趋势。

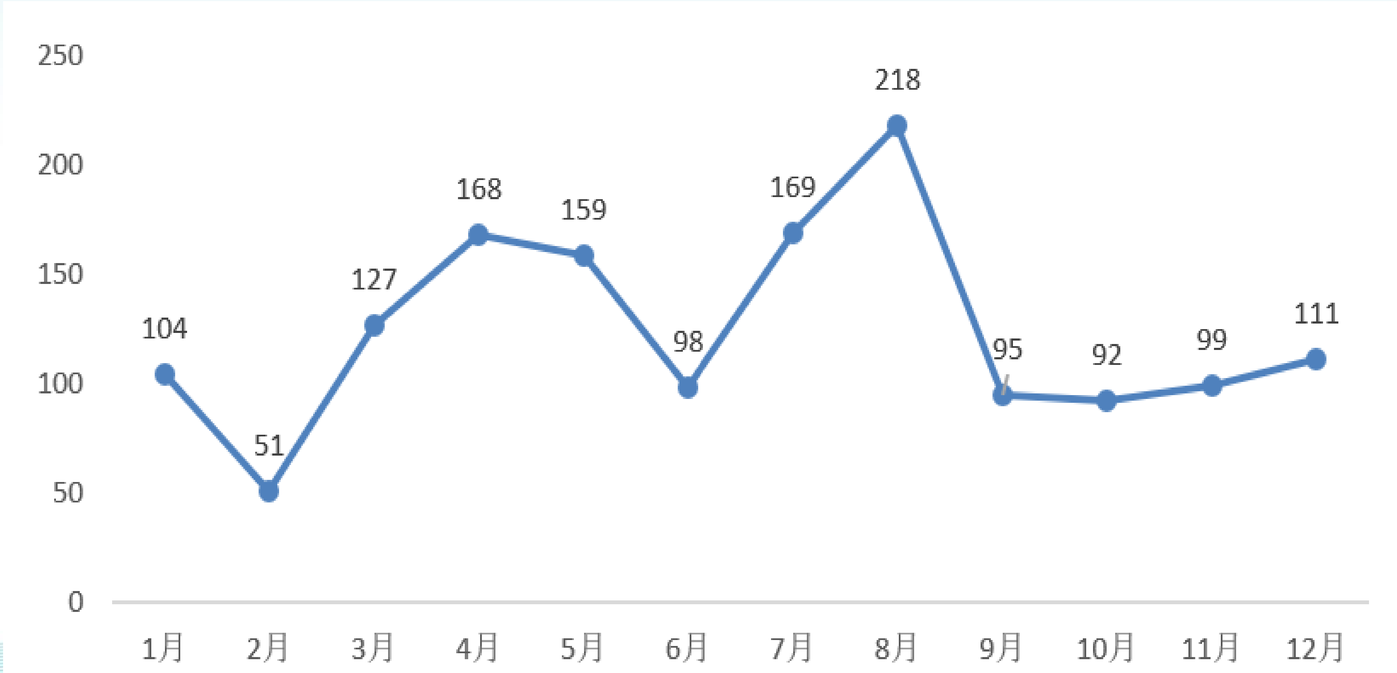
网站后门数据分析





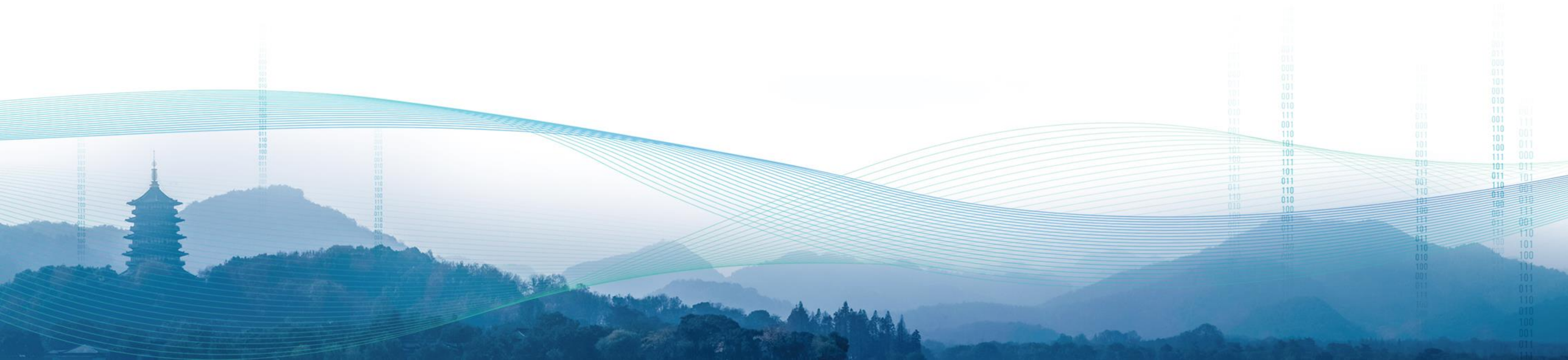
- 2018年全年，我国大陆地区被植入后门网站的数量为31,790个；
- 浙江省被植入后门网站数量1,491个，排名全国第六。

网站后门数据分析

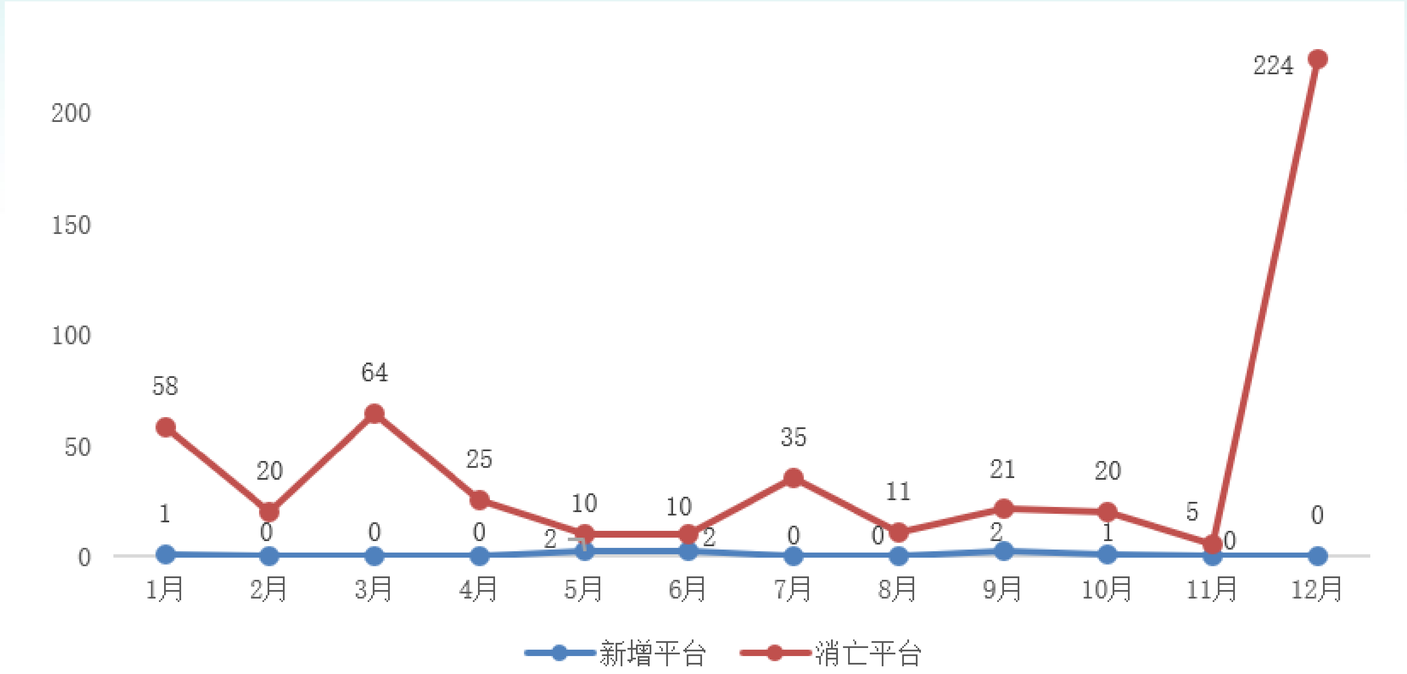


- 浙江省被植入后门网站从月度维度来看，8月份被植入后门网站数量最多，为218个，2月最少，为51个。

CONTENTS
目 录

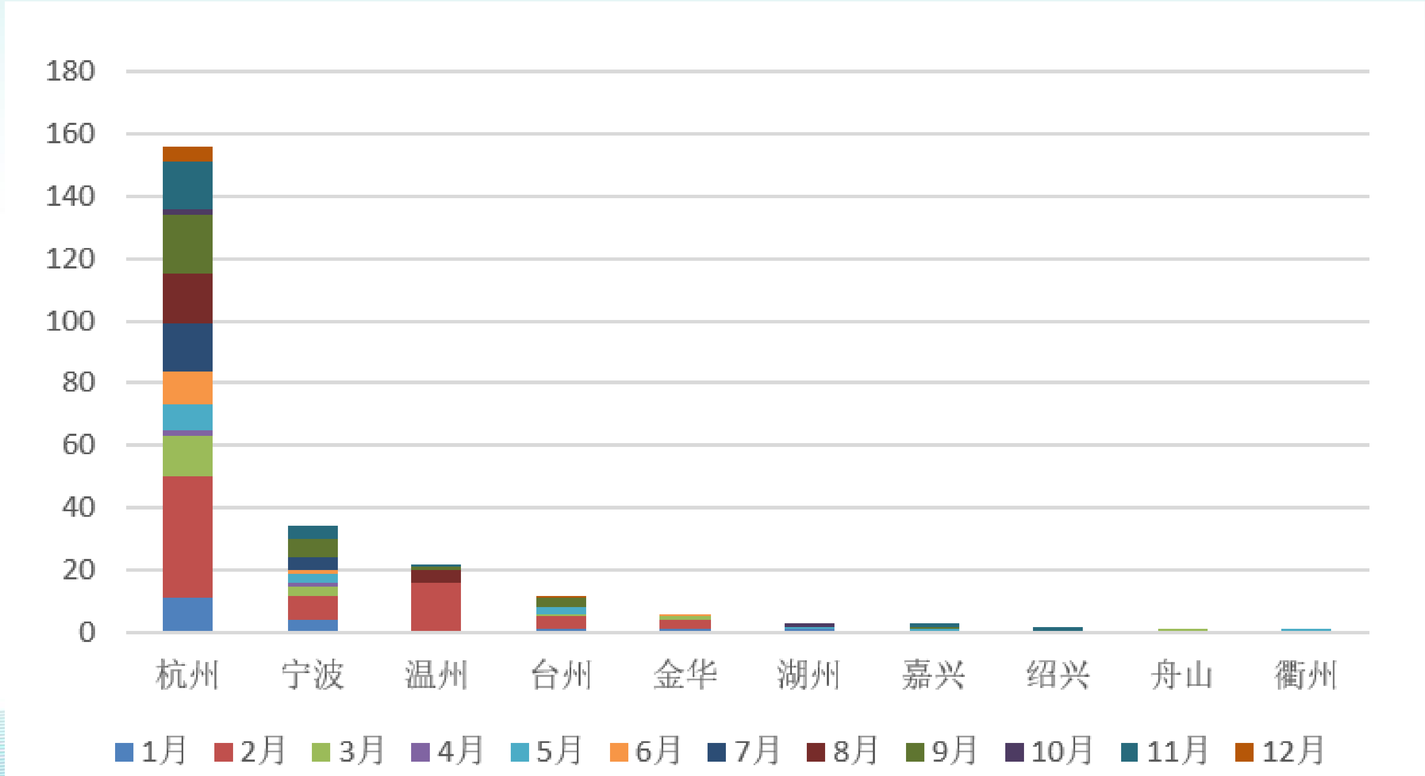


互联网金融专题-阶段发展情况



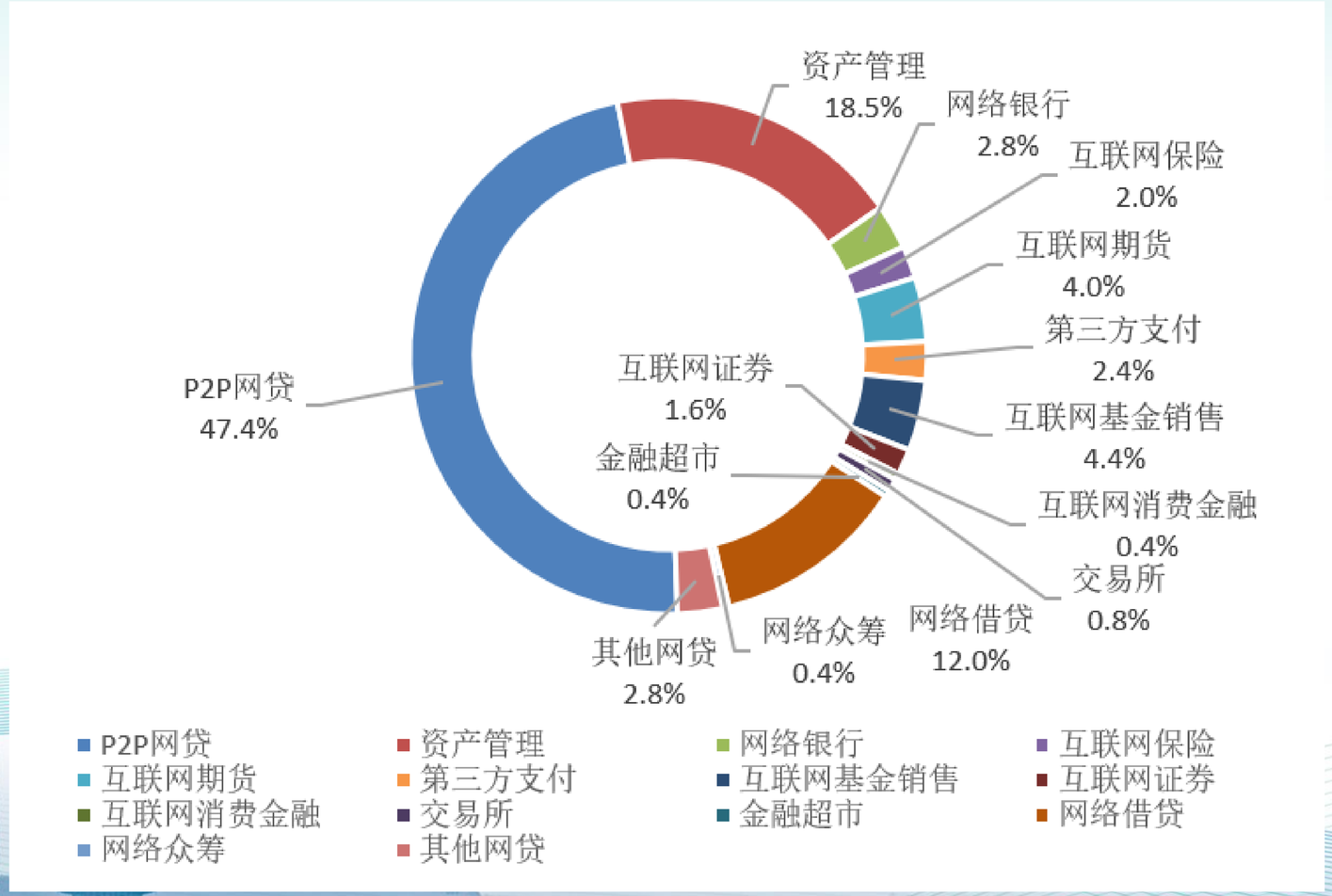
- 2018年全年，浙江省互联网金融平台累计数量达到3932家（不包括微盘），涉及20大类金融业态。
- 2018年全年，浙江省共新增平台8家，其中P2P网贷平台7家，互联网基金销售平台1家。全年，累计有503家平台已持续无法访问。

互联网金融专题-负面舆情情况



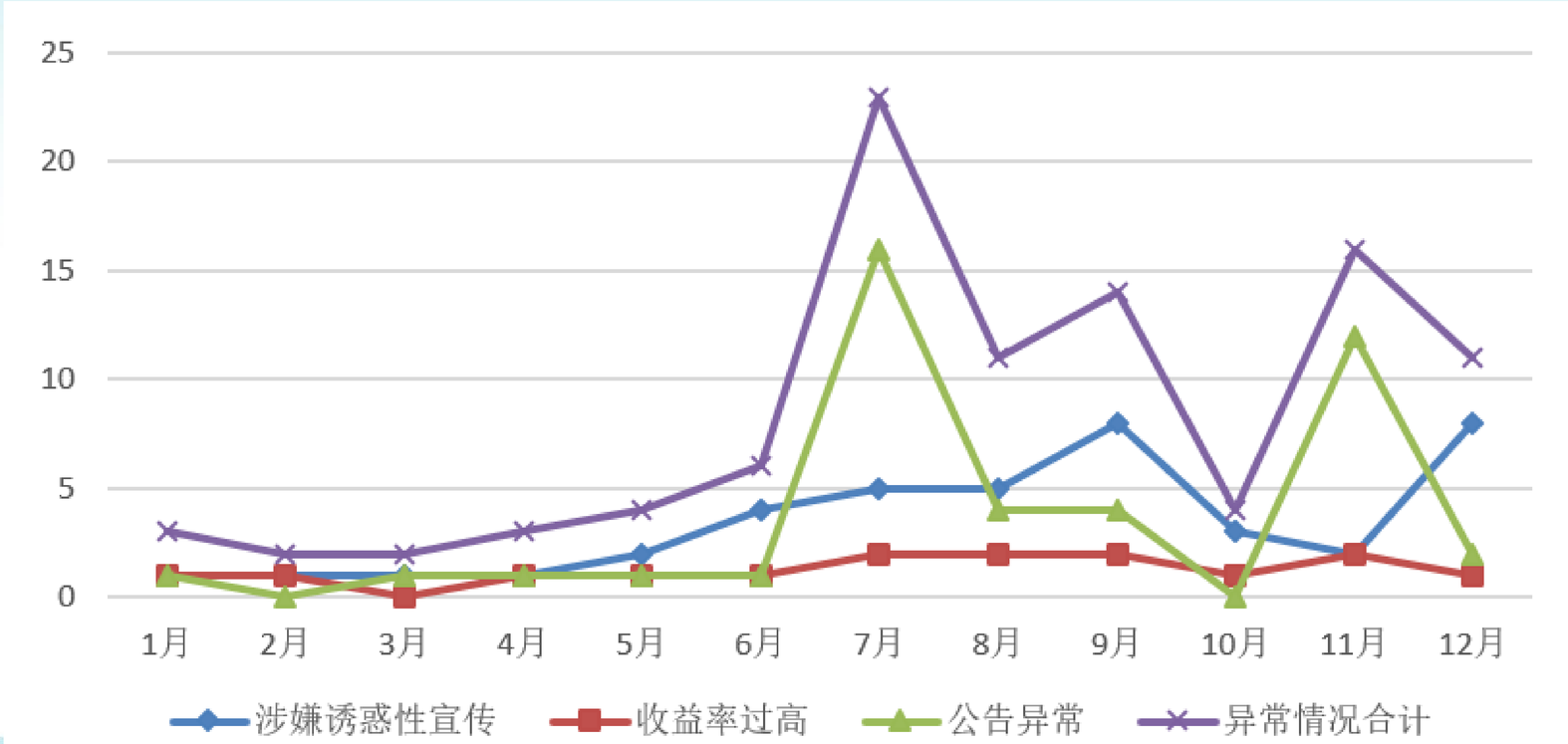
- 2018年全年，出现负面舆情的平台247家；
- 其中杭州156家（63.2%），宁波34家（13.8%）、温州22家（8.9%）。

互联网金融专题-负面舆情情况



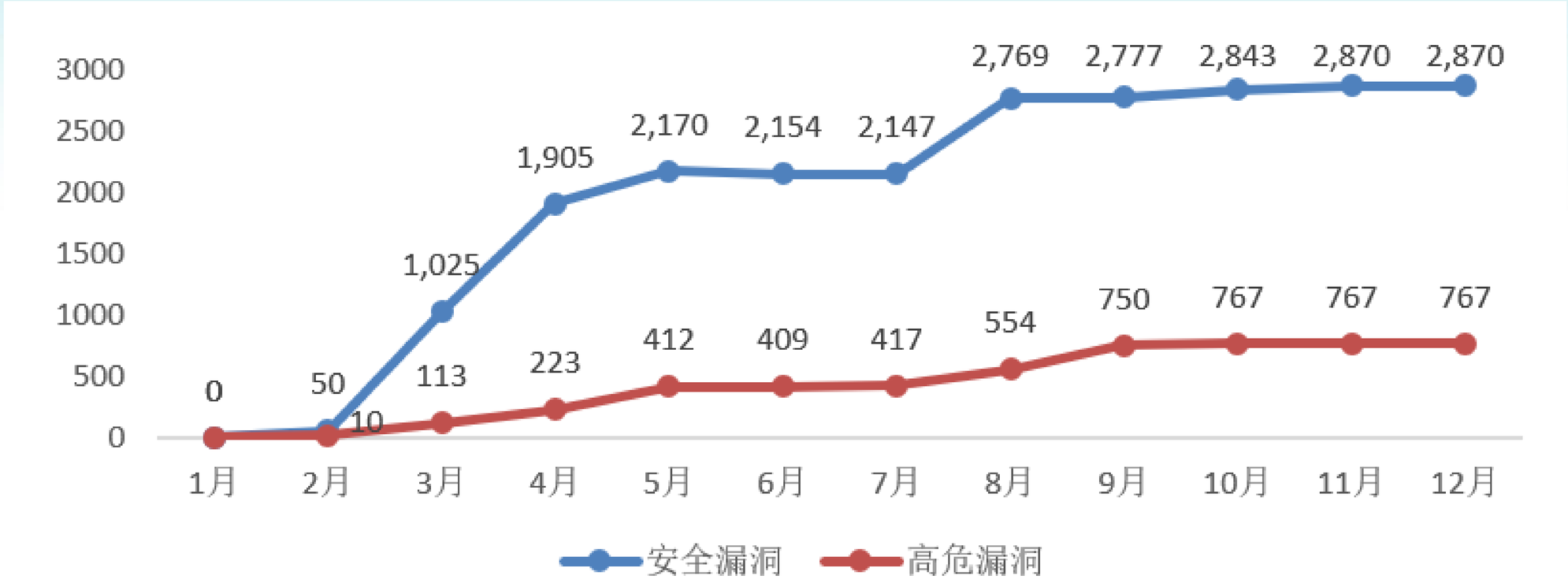
- **出现负面舆情的平台基本覆盖所有业态，其中P2P网贷、资产管理、网络借贷三种类型占比最高。**

互联网金融专题-负面舆情情况



- 2018年全年，浙江省对互联网金融平台涉嫌诱导性宣传、收益率过高、公告异常等3大类运行情况进行实时监测分析，全年发生的异常情况合计99件，其中涉嫌诱导性宣传41件，收益率过高15件，公告异常43件。

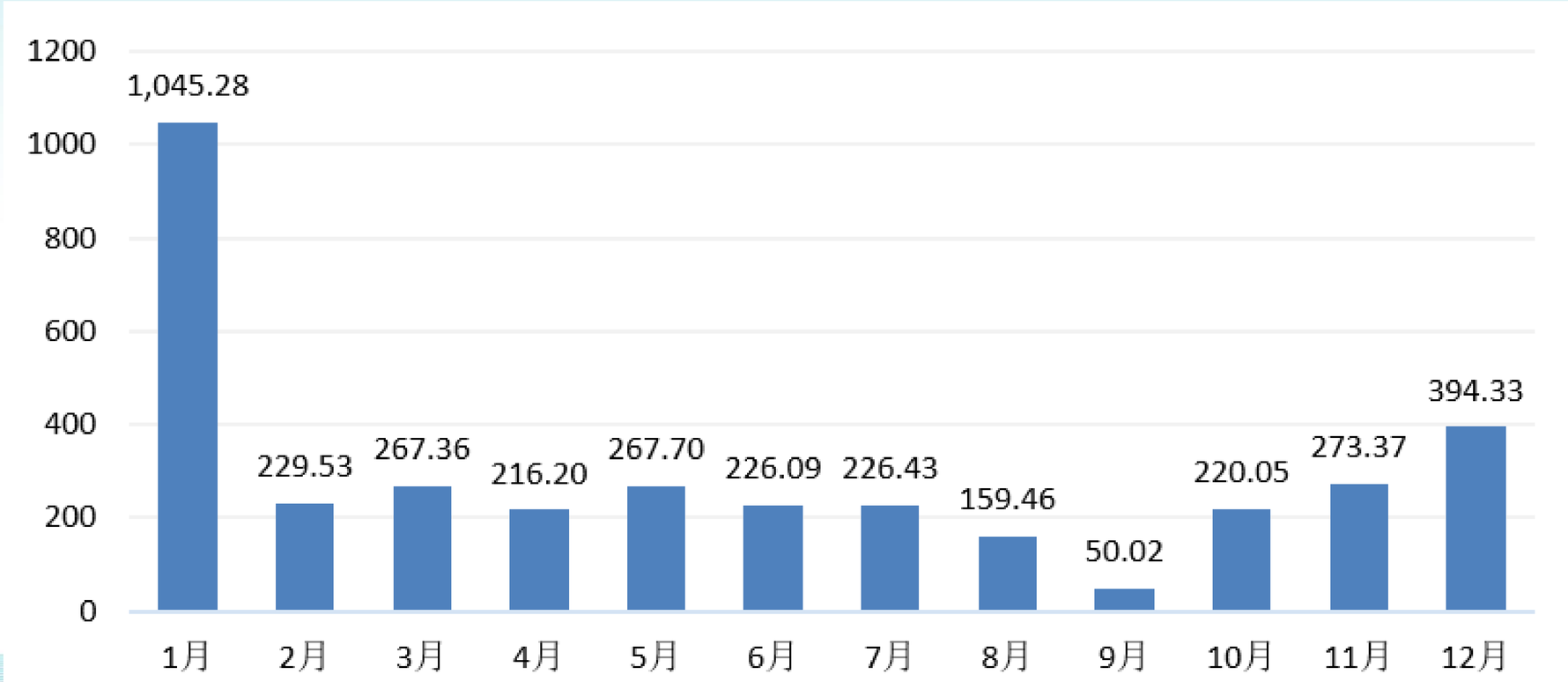
网络安全情况



- 2018年全年，共发现浙江省互联网金融网站漏洞23,580处，其中高危漏洞5,188处，约占总数22%；
- 高危漏洞类型主要以跨站脚本攻击漏洞及SQL注入漏洞为主，且呈增长趋势。

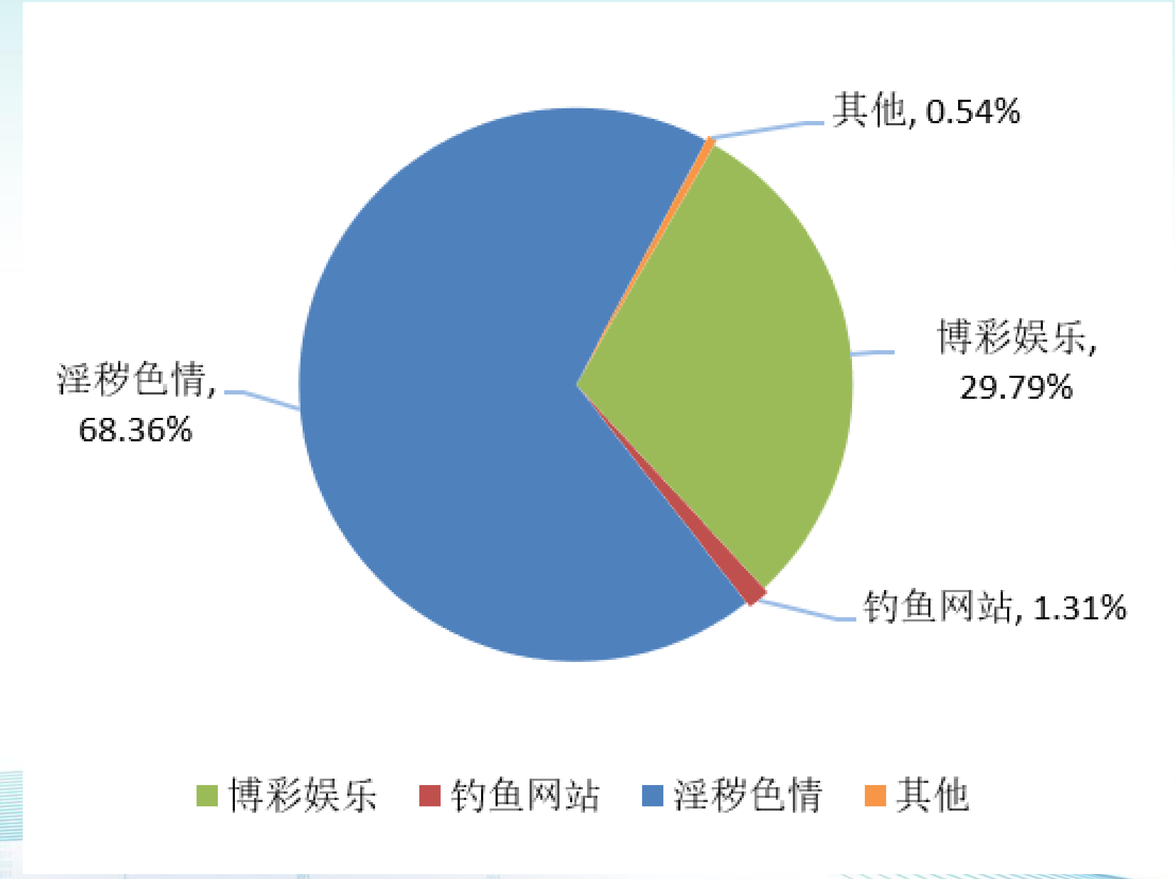
CONTENTS
目 录

新增恶意网站分析



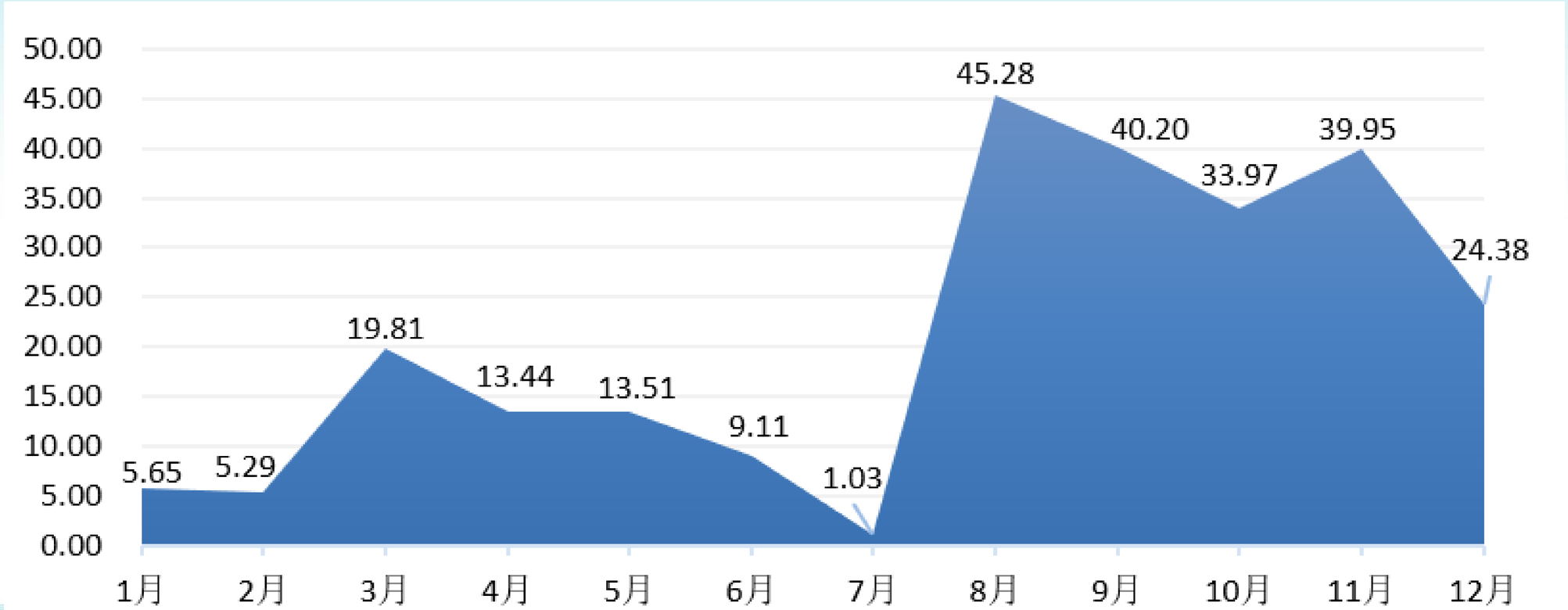
- 2018年检出浙江省恶意网址总量共3,575.82万个，平均每天检出量9.8万个；
- 1月份检出量1,045.28万个，为全年最多，其次是12月份检出量394.33万个。

新增恶意网站分析



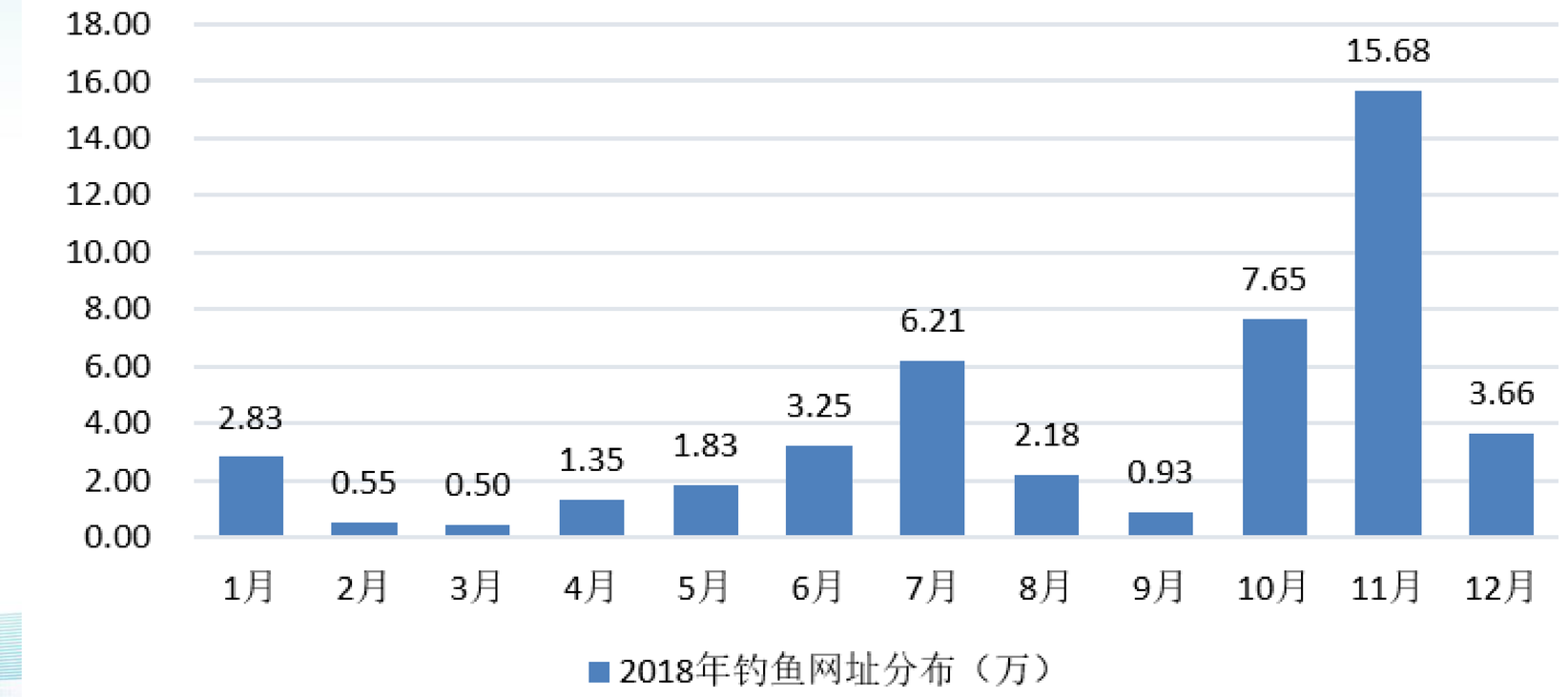
- 2018年浙江省恶意网址以淫秽色情、博彩娱乐和钓鱼网站为主，总比例已接近100%；
- 其中淫秽色情类型的网址占比68. 36%，为最高占比；
- 其次是博彩娱乐类型占比29. 79%；
- 钓鱼网站类型占比1. 31%。

新增恶意网站分析



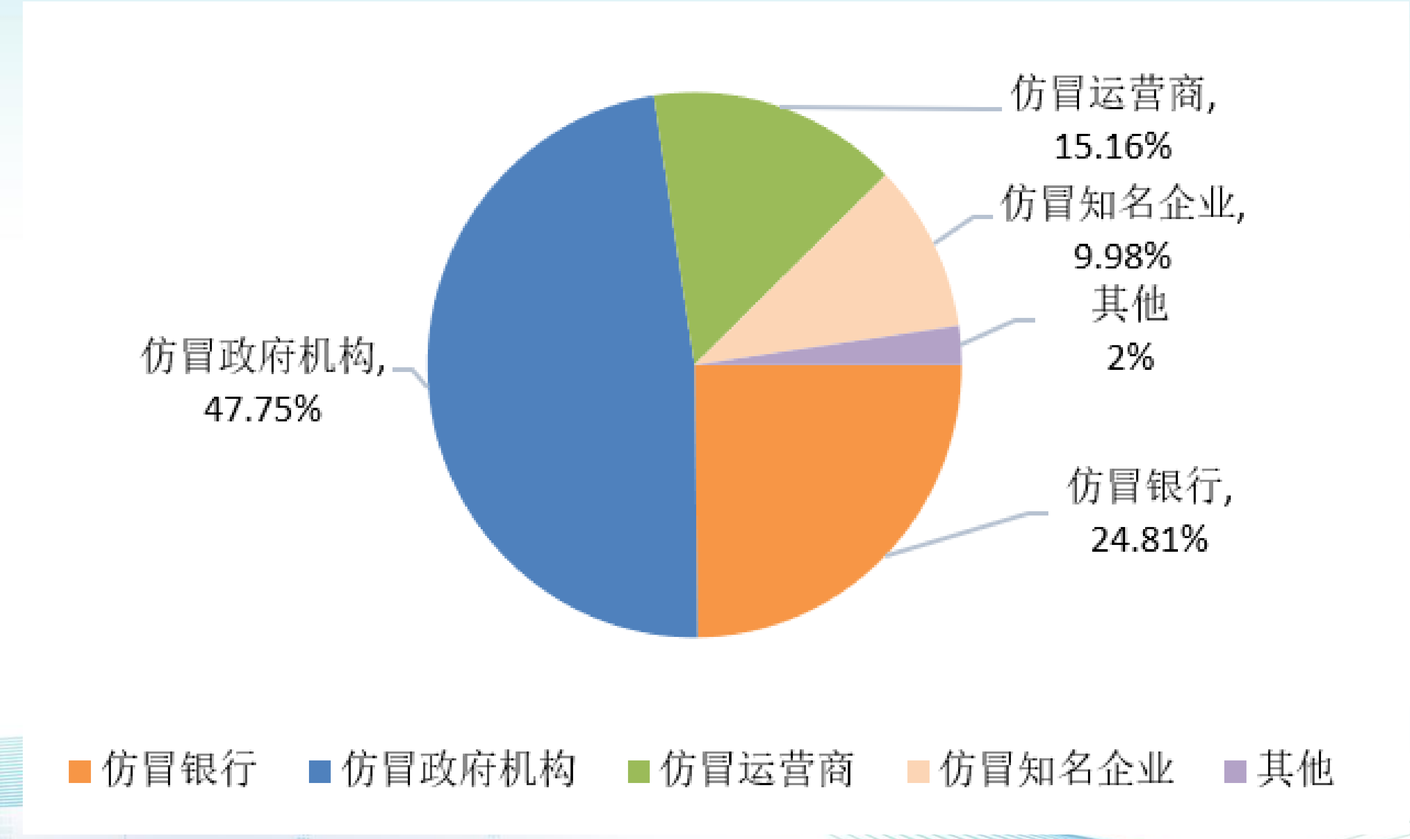
- 2018年浙江省固网、移动网用户访问恶意网址达251.61亿次；
- 其中8月访问45.28亿次，访问次数为全年最高；
- 其次为9月访问达40.2亿次，11月访问达39.95亿次。

钓鱼仿冒网站分析



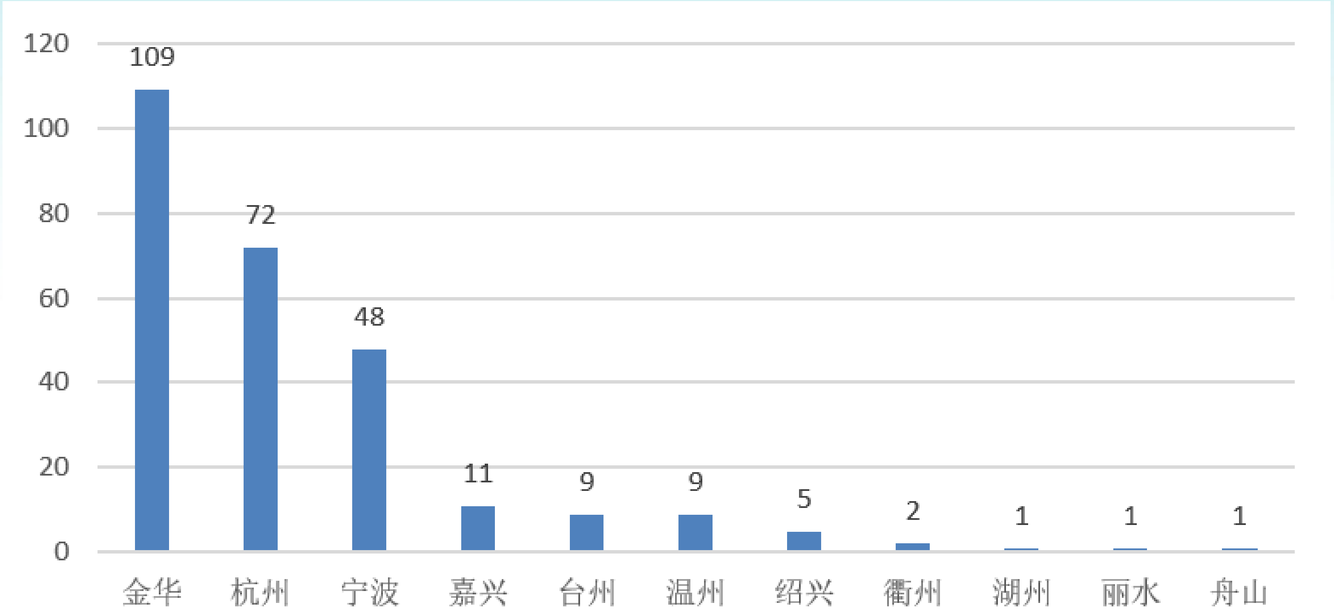
- 2018年浙江省钓鱼网站检出总量为46.62万个；
- 其中8月访问45.28亿次，访问次数为全年最高；
- 其次为9月访问达40.2亿次，11月访问达39.95亿次。

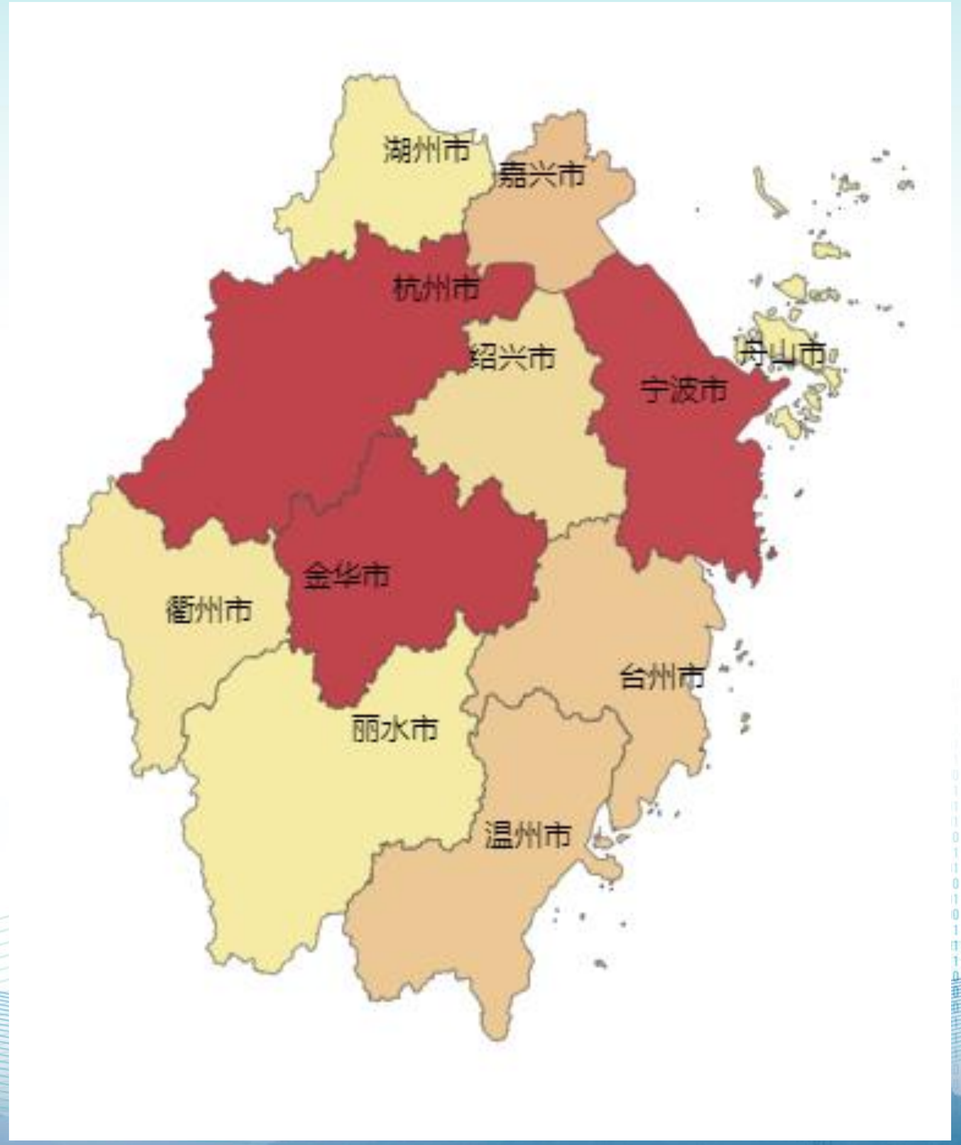
钓鱼仿冒网站分析



- 按照行业进行仿冒钓鱼网站监测，仿冒政府机构网站占比47. 75%，占比量最高；
- 其次是仿冒银行占比24. 81%；
- 仿冒运营商15. 16%。

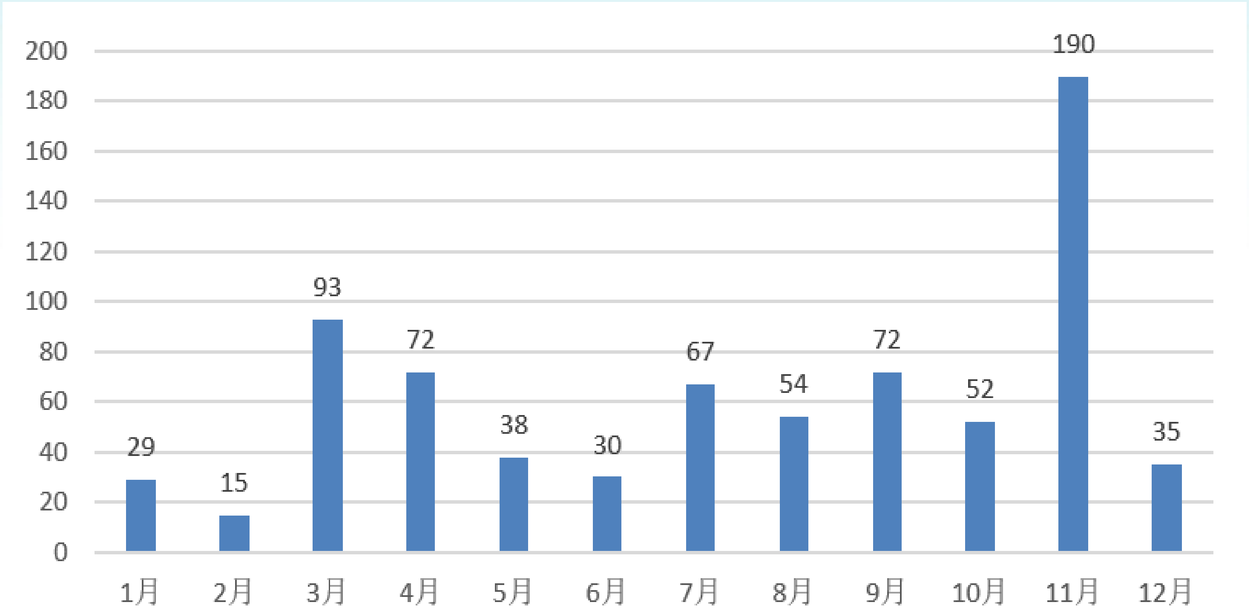
暴露联网设备

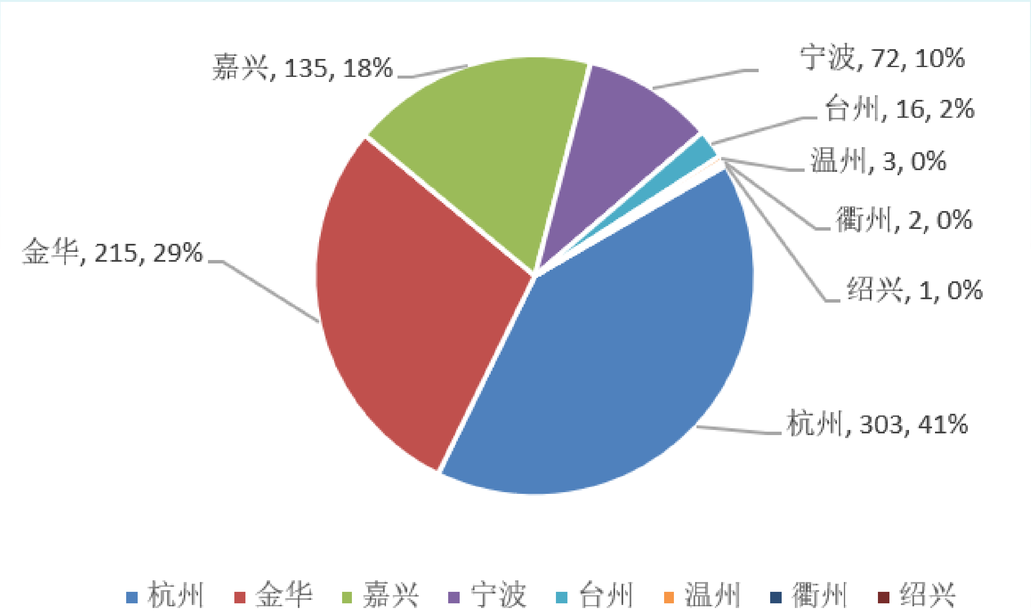




- 2018年通过无损探测，对全省范围内使用MODBUS、SNMP、EtherNet/IP、S7、FOX、FINS等协议的多种关键工控设备进行探测，发现识别设备268台，分布在全省10个地级市中；
- 其中暴露设备数量前三的城市为金华（109）、杭州（72）、宁波（48）。

安全监测





- 2018年，累计监测到境外组织对浙江省联网工控设备的探测响应事件共计747起；
- 共涉及省内杭州、金华、宁波、温州和绍兴等8个城市。

CONTENTS
目 录

涵盖的业务范围

互联网安全

- 网络钓鱼监测处置服务
- 互联网关口监测服务
- 安全漏洞通报服务
- DDoS监测处置服务

安全评估

- 安全评估服务
- 渗透测试服务
- 代码审计服务
- 攻击路径检测

移动互联网安全

- 仿冒app监测处置服务
- App安全风险评估服务

涵盖的业务范围

产品测试

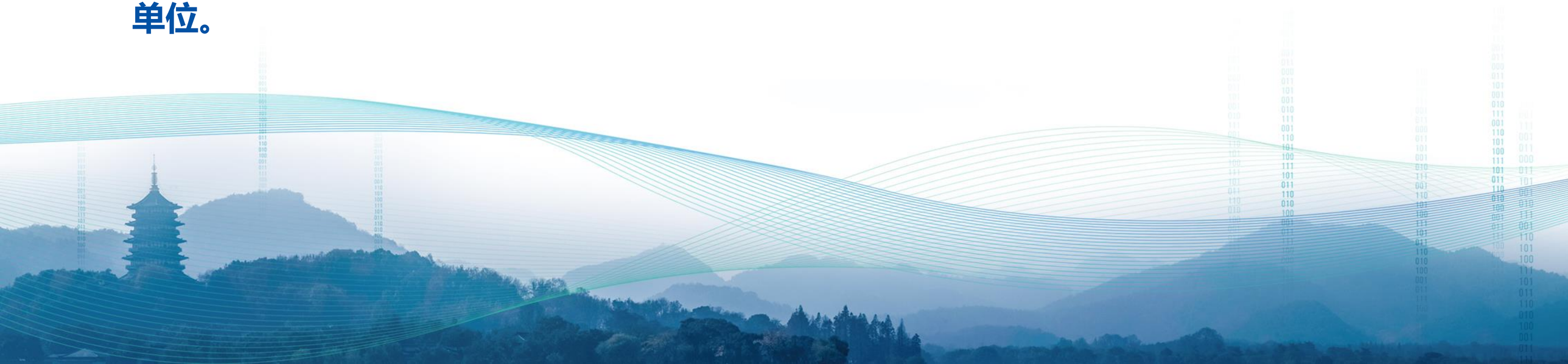
- 网络设备测评服务
- 安全设备测评服务
- 信息安全产品分级评估

网络舆情和人才培养

- 全方位的专业舆情分析服务
- 网络信息安全培训（CCSRP）

ZJCERT情况介绍

国家计算机网络应急技术处理协调中心浙江分中心（以下简称“ZJCERT”）成立于2002年，是国家计算机网络应急技术处理协调中心在浙江的分支机构，为副厅级公益二类事业单位。



ZJCERT网络安全主要职责

- 承担网络安全监测预警、事件处置、应急演练等技术支撑工作
- 承担关键信息基础设施和重要信息系统的网络安全检查、风险评估、等级保护评测、安全防护等技术支撑工作
- 承担互联网新技术、新业务、新业态安全风险问题的技术研究、测试评估工作；为所在地信息化发展提供安全技术支撑服务
- 负责统筹协调对外服务与合作

THANK YOU

谢　　谢　　观　　看