江苏省互联网网络安全报告
（2017年度）

江苏省通信管理局

江苏省互联网应急中心

江苏省互联网行业管理服务中心

2018年4月

《2017年度江苏省互联网网络安全报告》
编制人员名单

总　　编：袁瑞青

副 总 编：王云飞

编写成员：任光裕　　马　旸　　刘明芳　　仲思超

蔡　冰　　尹魏昕　　罗雅琼　　韦芹余

邱凌志　　顾　弘　　胡　鹏　　熊逸文

前言

为真实有效地反映江苏省互联网网络安全状况，给政府部门、关键信息基础设施运营单位、通信运营企业、增值电信企业以及全省网民提供网络安全态势的宏观分析及预测，江苏省通信管理局、国家计算机网络与信息安全管理中心江苏分中心（中文简称江苏省互联网应急中心，英文简称 CNCERT/JS）自2009年开始每年撰写和发布《江苏省互联网网络安全报告》。

《2017 年度江苏省互联网网络安全报告》分析了国家互联网应急中心、江苏省通信管理局、江苏省互联网应急中心自有的网络安全监测数据，汇总了江苏省通信运营企业、全国网络安全企业等相关单位报送的信息，具有鲜明的行业特色。报告分析了 2017 年江苏省网络安全宏观形势，涉及网站安全、主机安全、移动互联网安全等多个安全领域，对国内发生的各类网络安全事件进行多维度的统计分析，并深入剖析了典型的网络安全案例，针对性地提出网络安全防护对策建议，希望本报告能对提升江苏省互联网网络安全防护水平起到积极的促进作用。

本报告撰写过程中，中国电信股份有限公司江苏分公司、中国移动通信集团江苏有限公司、中国联合通信有限公司江苏省分公司、北京天融信科技股份有限公司、360 企业安全（网神信息技术（北京）股份有限公司）、哈尔滨安天科技集团股份有限公司、启明星辰信息技术集团股份有限公司、恒安嘉新（北京）科技股份公司、南京铱迅信息技术股份有限公司等单位提供了数据素材，在此一并致谢。

由于水平有限，本报告难免存在疏漏和欠缺。我们诚挚地希望广大读者、业界同仁不吝赐教，提出宝贵意见。

江苏省通信管理局

江苏省互联网应急中心

江苏省互联网行业管理服务中心

2018 年 4 月

目录

1、江苏省互联网网络安全总体状况.....1
1.1 网络安全形势.....2
1.2 数据导读.....5
2、计算机恶意程序传播和活动情况.....7
2.1 僵尸木马受控端情况.....7
2.2 僵尸木马控制端情况.....10
2.3 飞客蠕虫病毒感染情况.....12
3、移动互联网恶意程序感染情况.....15
3.1 移动互联网恶意程序传播和活动情况.....15
3.2 移动互联网恶意程序感染情况.....16
3.3 移动互联网恶意程序行为属性.....17
3.4 移动互联网恶意程序感染平台分析.....18
3.5 移动互联网恶意程序感染用户 TOP10.....18
4、网站安全监测情况.....20
4.1 网页篡改事件.....20
4.2 网站后门事件.....22
4.3 网页仿冒事件.....24
4.4 网页挂马事件.....27
4.5 网站类安全事件处置建议.....30
5、安全漏洞监测情况.....31
5.1 重要信息系统漏洞威胁情况分析.....31
5.2 WANNACRY 勒索病毒席卷全球.....32
5.3 全省传播感染情况分析.....35
6、网络安全专题分析.....39
6.1 网络安全威胁治理专题.....39
6.2 工业互联网安全专题.....40
6.3 DDOS 攻击事件专题.....43
6.4 物联网设备安全专题.....47
6.5 APT 攻击事件专题.....50
7、重点行业互联网安全状况分析.....55
7.1 党政机关互联网安全状况.....55
7.2 金融行业互联网安全状况.....61
7.3 教育行业互联网安全状况.....63
8、2017 年网安热点及 CNCERT/JS 重点工作.....64
8.1 国际国内热点问题.....64
8.2 2017 年 CNCERT/JS 重点工作.....66
8.3 江苏省网络安全组织发展情况介绍.....70
9、2017 年网络安全态势分析及 2018 年趋势预测.....75
9.1 2017 年网络安全态势分析.....75
9.2 2018 年网络安全趋势预测.....78

1、江苏省互联网网络安全总体状况

当前，网络空间已经成为现代国家的新疆域、全球治理的新领域，网络安全渗透到政治、经济和社会发展的方方面面，十九大报告再次提出要建设网络强国、数字中国、智慧社会，并多处提及互联网和网络安全。这是继 2016 年 4 月 19 日网络安全和信息化工作座谈会并发表重要讲话之后，习近平总书记再次从国家总体宏观战略的高度，为网信工作的下一步开展指明了方向。

在习总书记系列讲话精神和新发展理念指引下，2017 年我国互联网治理法治化进程日新月异，取得的成就也非常显著，2017 年 6 月 1 日，《中华人民共和国网络安全法》正式实施，不仅从法律上保障了公民在网络空间的利益，有效维护了国家网络空间主权和安全，还有利于信息技术的应用，有利于发挥互联网的巨大潜力；6 月 27 日，中央网络安全和信息化领导小组办公室印发了《国家网络安全事件应急预案》；9 月和 11 月，工业和信息化部先后制定印发了《公共互联网网络安全威胁监测与处置办法》和《公共互联网网络安全突发事件应急预案》。

2017 年是全面实施“十三五”规划的重要一年，是全面建成小康社会的加速之年，是全面深化改革向纵深推进的关键一年。截止 2017 年底，我省网民规模已达 4903 万，网民普及率达到 61.1%，手机网民数 4827 万，手机网民在网民中占比 98.4%。全省域名总数达 161.61 万个，同比减少了 6.7%，占全国域名总数的 4.2%，居全国第六位，排名与 2016 年持平。固定互联网宽带接入用户数为 3106.2 万户，同比增长 15.7%。

互联网行业高速发展的同时，网络安全问题仍然高悬于顶。2017 年爆发的 CIA 黑客工具“Vault 7”泄露、NSA“方程式小组”黑客工具泄露、蠕虫勒索软件袭击等网络安全事件震惊世界；英特尔、博通等曝光的底层漏洞动辄影响数十亿设备；针对我国境内目标关键信息基础设施发动攻击的 APT 组织已达 38 个；2017 年全省遭到攻击流量在 1Gbps 以上的 DDoS 攻击次数达 17.87 万次，最高攻击峰值达到 575.27Gbps；全年我省僵尸木马、飞客蠕虫、网页篡改、网站后

门、网页仿冒、网页挂马、移动互联网恶意程序等网络安全事件数仍居全国前列，这些都值得全省网民高度重视。

1.1 网络安全形势

1.1.1 党对网信工作的领导全面加强

（1）党的十九大报告深入阐述网络安全问题

2017 年 10 月 18 日，中国共产党第十九次全国代表大会在北京人民大会堂开幕。习近平总书记代表第十八届中央委员会向大会作报告，报告指出：“互联网建设管理运用不断完善”、“加强互联网内容建设，建立网络综合治理体系，营造清朗的网络空间”、“增强改革创新本领，保持锐意进取的精神风貌，善于结合实际创造性推动工作，善于运用互联网技术和信息化手段开展工作”。

报告气势恢弘、催人奋进、高屋建瓴、主题明确、意义深远，制定了新时代中国特色社会主义的行动纲领和发展蓝图，提出要建设网络强国、数字中国、智慧社会，推动互联网、大数据、人工智能和实体经济深度融合，建立网络综合治理体系，营造清朗的网络空间，提高基于网络信息体系的联合作战能力等。

党的十八大以来，在党中央坚强领导下，各地各部门锐意创新、多措并举，开创了互联网发展、治理新局面，百姓在共享互联网发展成果上有了更多获得感，网信事业发展实现新跨越。站在新的历史起点上，在习近平新时代中国特色社会主义思想指引下，我国正以更自信、更有力、更坚定、更迅疾的步伐，向网络强国新时代昂首迈进。

（2）网信事业必须始终贯彻以人民为中心的发展思想

在我国网信事业发展进入新的历史时期的关键转折点，2016 年 4 月 19 日，习近平总书记在网络安全和信息化工作座谈会上强调：“网信事业要发展，必须贯彻以人民为中心的发展思想”。一年过去，随着全面从严治党的不断推进，再次认真学习习近平总书记在网络安全和信息化工作座谈会上的重要讲话时，越来越多的人形成了一个强大共识：要确保我国网信事业在新的历史起点上实现更好更快地发展，就必须始终贯彻以人民为中心的发展思想，这样才能让互联网更好造福人民。

中国共产党的根本宗旨决定了网信事业必须贯彻以人民为中心的发展思想。以人民为中心的发展思想是中国社会主义革命、建设取得巨大成就的成功之基、

制胜法宝，是在网络时代对全心全意为人民服务的新诠释，是全面从严治党的有力抓手和重要展现，是否真正坚持以人民为中心的发展思想是检验共产党人的试金石。

（3）网络安全工作得到各级党委（党组）重视和加强

网络安全工作事关国家安全、政权安全和经济社会发展。为进一步加强网络安全工作，全面落实网络信息安全主体责任，提高网络信息安全防护能力，2017 年，江苏省各级党委政府陆续成立各自的网络信息安全工作领导小组，明确和落实党委（党组）领导班子、领导干部网络安全责任，根据《中国共产党问责条例》、《中央网络安全和信息化领导小组工作规则》等有关规定，按照谁主管谁负责、属地管理的原则，各级党委（党组）对本地区本部门网络安全工作负主体责任，领导班子主要负责人是第一责任人，主管网络安全的领导班子成员是直接责任人。各级党委（党组）违反或者未能正确履行职责，将按照有关规定追究其相关责任。

（4）江苏正式成立省委网信办

2017年11月1日下午，江苏省委网信办召开全体干部会议，省委常委、宣传部部长王燕文同志出席会议并讲话。

王燕文同志强调，全省网信系统干部要始终坚定自觉地同以习近平同志为核心的党中央保持高度一致，认清肩负的使命责任，抓住新机遇，把握新要求，推动我省网信工作再上新台阶。一是要强化“四个意识”，切实把牢方向导向；二是要创新方式方法，确保网上正能量强劲；三是要加强阵地管理，切实落实属地责任；四是要注重统筹协调，形成工作强大合力；五是要坚持从严要求，建设过硬领导班子和干部队伍。

王燕文指出，新成立的省委网信办是一个新机构，网信队伍是一支新队伍，年轻人多，要切实提高素质能力，努力在新时代、新起点上开创工作新局面，为推进“两聚一高”新实践、建设“强富美高”新江苏作出新的更大贡献。

1.1.2 公共互联网网络安全状况

2017 年，据江苏省互联网应急中心自主监测，江苏省互联网网络安全状况总体平稳，未发生重大网络安全事件。通过长期的专项整治，僵尸木马控制、网页篡改、网页仿冒等事件数量均有所下降。

（1）木马和僵尸网络

据监测，江苏省木马僵尸网络控制端和受控端主机数量双双下降，但受控事件数量有所提升，尤其是随着境内控制端的精确打击，境外木马和僵尸网络控制端比例持续增长，绝大部分控制端来自美国、韩国等地。来自于美国的1936个IP地址控制了江苏省17.94万个IP地址，占总受控IP地址数的29.04%，控制频次全年达5.84亿次，占全省受控事件数的54.84%。

（2）移动互联网恶意程序

移动互联网恶意程序数量已连续多年持续增长，CNCERT/CC全年通过监测和厂商交换获得恶意程序样本253.33万个，较2016年上涨23.36%。从行为属性方面统计，流氓行为、恶意扣费、资费消耗及隐私窃取类移动互联网恶意程序位居前列；从危害性方面统计，高危、中危及低危病毒占比分别为1.27%、9.54%、89.19%。据江苏省互联网应急中心监测发现，2017年江苏省用户感染的移动恶意程序事件数量较上年有明显下降，恶意类型主要集中在“流氓行为”，数量达91.00万个，占总数的35.92%。经过江苏省互联网应急中心连续四年的治理，省内主流应用商店积极落实安全责任，不断完善安全检测、安全审核、社会监督举报、恶意程序下架等制度，积极参与处置响应与反馈，恶意APP下架数量连续保持下降趋势，大量移动互联网恶意程序的传播渠道转移到网盘或广告平台等网站。

（3）拒绝服务攻击

拒绝服务攻击（DDoS攻击）指黑客组织通过控制服务器、肉鸡等资源，发动对包括国家骨干网络、重要网络设施、政企或个人网站在内的互联网上任一目标攻击，致使目标服务器无法提供正常服务。2017年美国对外发起的DDoS攻击数量最多，占全球DDoS攻击总事件的37.06%；而中国则成为了遭受DDoS攻击的重灾区，占全球DDoS攻击数量的84.79%。据基础电信企业报送，2017年我省攻击流量在1Gbps以上的DDoS攻击次数达17.87万次，日均攻击次数达到489次，攻击流量最高达到575.27Gbps，我省多个政府网站和新闻门户网站遭受攻击。经江苏省互联网应急中心协调，为我省212个重要信息系统提供网站云防护，全年均未发生重大网络安全事件。

（4）安全漏洞

2017 年，国家信息安全漏洞共享平台（CNVD）共收录通用软硬件漏洞 15955 个。其中，高危漏洞 5615 个、中危漏洞 9219 个、低危漏洞 1121 个，较 2016 年增长 47.43%。在全年收录的漏洞中，有 3854 个“0day”漏洞，可用于实施远程网络攻击的漏洞有 14158 个。全年，江苏省互联网应急中心共监测发现江苏省各级党政机关、高校、医院网站及其他重要信息系统存在各类网站漏洞 1131 个，省级单位存在安全漏洞 195 个，设区市级存在安全漏洞 610 个，区县及以下存在安全漏洞 326 个。

1.1.3 网络安全横向合作

习近平指出：“金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标”，“不出问题则已，一出就可能导致交通中断、金融紊乱、电力瘫痪等问题，具有很大的破坏性和杀伤力”。因此，面向公共互联网的应急处置工作逐步成为公共应急服务事业的重要组成部分，建立高效的公共互联网应急体系和强大的人才队伍，对及时有效地应对互联网突发事件有着重要意义。为拓宽掌握互联网宏观网络安全状况和网络安全事件信息的渠道，增强对重大突发网络安全事件的应对能力，强化公共互联网网络安全应急技术体系建设。促进互联网网络安全应急服务的规范化和本地化，江苏省通信管理局、江苏省互联网应急中心、江苏省通信行业协会及江苏省互联网协会在多维度多层面构建了共有 20 家互联网应急支撑单位、50 家信息通报成员单位和 39 家网络安全专业委员会成员单位组成的网络安全应急支撑体系。

1.2 数据导读

以下是对 2017 年江苏省网络安全状况主要数据的导读分析：

（1）木马僵尸程序监测

2017 年，江苏省木马和僵尸程序控制服务器 IP 地址总数为 2647 个，同比下降 19.96%，僵尸木马控制端与其他主机通信 1.28 亿次，同比下降 30.43%。2017 年，江苏省受控主机 IP 地址总数为 37.75 万个，同比下降 69.80%，境内外主机与受控“肉鸡”通信 10.65 亿次，其中境外主机与受控“肉鸡”通信占 87.32%。

（2）飞客蠕虫感染情况监测

2017 年，江苏省感染飞客蠕虫病毒事件 554.36 万起，较 2016 年上升 99.92%，涉及 25.57 万个 IP 地址，较 2016 年下降 44.98%。

（3）移动互联网安全监测

2017 年，CNCERT/CC 监测发现移动互联网恶意程序新型样本数量为 253.33 万个，同比增长 23.36%。全年江苏省用户感染各类移动互联网恶意程序事件 4779.64 万起，月均 31.36 万个用户感染；按行为属性统计，2017 年“恶意扣费”类恶意程序数量已跃居首位，感染用户数为 244.06 万个，占 63.17%；按操作系统分布统计，使用 Android 平台的用户感染恶意程序事件为 4775.98 万起，占 99.67%，约有 371.24 万使用 Android 平台的用户感染病毒。

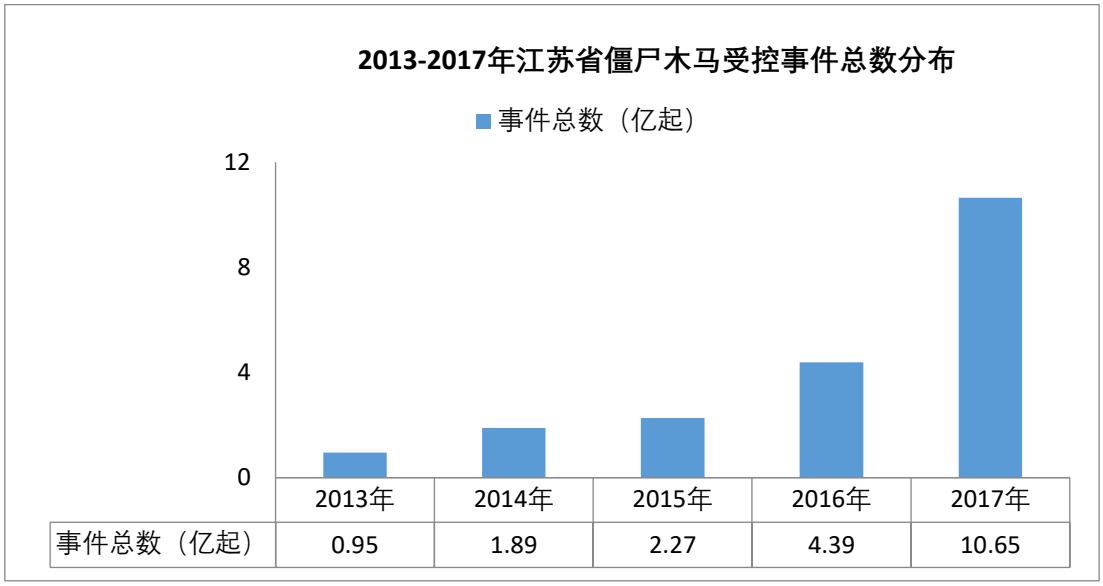
（4）网站安全监测

2017 年，全省共发生网站篡改事件 6045 起，同比下降 36.84%，全省共有 382 个网站遭受篡改，其中遭受篡改网站数最多的设区市是苏州，达 77 个；全省 1163 个网站被植入后门，域名后缀为.com 的网站最多，数量达 621 个，其中网站被植入后门数最多的设区市是南京，占 17.19%；网页仿冒事件 9013 起，同比下降 26.16%，其中“虚假购物”类型的仿冒事件最多，占总数的 43.25%；网页挂马事件 8.19 万起，同比下降 68.01%。

2、计算机恶意程序传播和活动情况

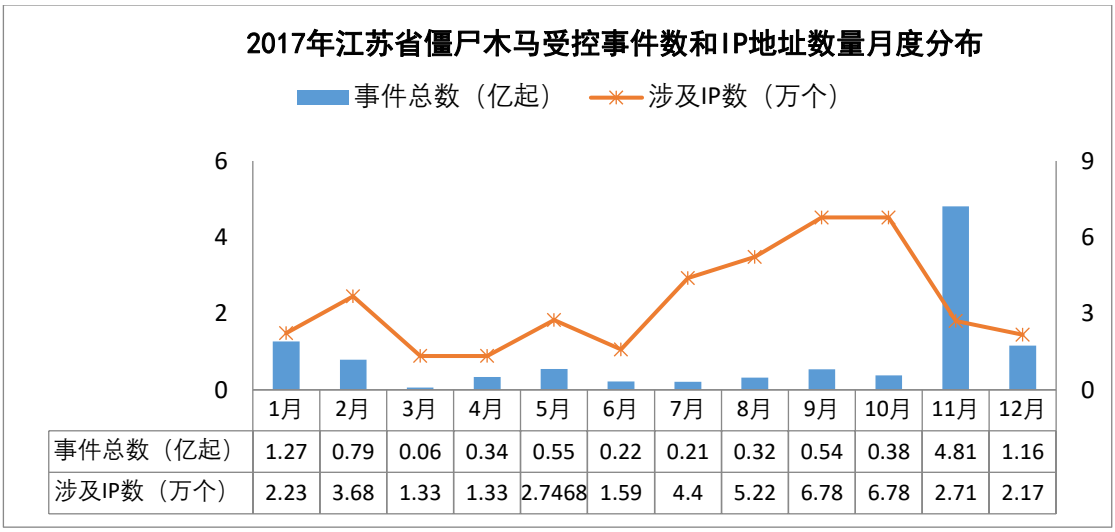
2.1 僵尸木马受控端情况

2017 年，江苏省互联网主机遭僵尸木马恶意控制的事件 10.65 亿起，涉及受控 IP 地址 37.75 万个，同比下降 69.80%。2013 至 2017 年江苏省僵尸木马受控事件总数分布如图 2.1 所示。2017 年江苏省僵尸木马受控事件数及 IP 地址数月度分布如图 2.2 所示。



	2013年	2014年	2015年	2016年	2017年
事件总数（亿起）	0.95	1.89	2.27	4.39	10.65

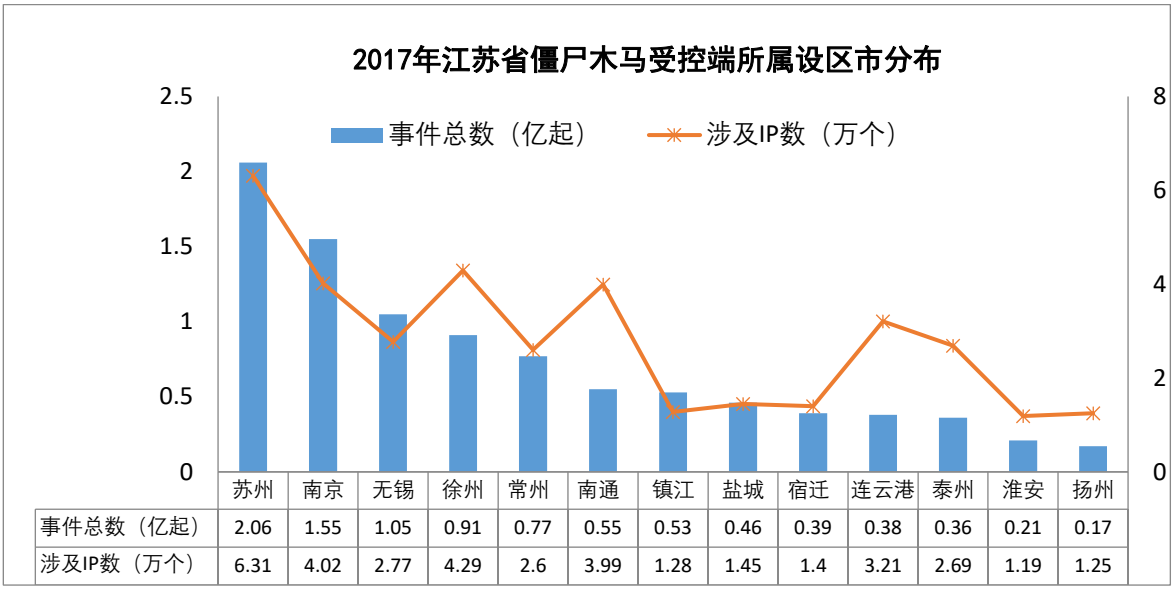
图 2.1 2013-2017 年江苏省僵尸木马受控事件总数分布图



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
事件总数（亿起）	1.27	0.79	0.06	0.34	0.55	0.22	0.21	0.32	0.54	0.38	4.81	1.16
涉及IP数（万个）	2.23	3.68	1.33	1.33	2.7468	1.59	4.4	5.22	6.78	6.78	2.71	2.17

图 2.2 2017 年江苏省僵尸木马受控事件数和 IP 地址数量月度分布图

【受控主机所属设区市分布情况】2017 年，江苏省僵尸木马受控主机主要分布在苏州、徐州和南京，2017 年江苏省僵尸木马受控端所属设区市分布如图 2.3 所示。



	苏州	南京	无锡	徐州	常州	南通	镇江	盐城	宿迁	连云港	泰州	淮安	扬州
事件总数（亿起）	2.06	1.55	1.05	0.91	0.77	0.55	0.53	0.46	0.39	0.38	0.36	0.21	0.17
涉及IP数（万个）	6.31	4.02	2.77	4.29	2.6	3.99	1.28	1.45	1.4	3.21	2.69	1.19	1.25

图 2.3 2017 年江苏省僵尸木马受控端所属设区市分布图

【TOP10 受控木马类型分析】僵尸木马受控事件中，通过感染木马-远控-Trojan.Win32.FakeLPK.7cfa、木马-远控-Worm.Agent.qub-2、木马-远控-白金远控-基础 1、木马-远控-白金远控-基础 2 等病毒而被控制的事件数最多，分别为 3.79 亿起、1.26 亿起、9502.14 万起、8967.09 万起。实际受控 IP 地址中，感染木马-远控-Trojan.Win32.FakeLPK.7cfa、僵尸网络-其他协议-IMDDOS_2、木马-远控-白金远控-基础 1、木马-远控-白金远控-基础 2 等病毒而被控的 IP 地址数最多，分别为 13.59 万个、11.44 万个、2.76 万个、2.72 万个。受控端感染病毒 TOP10 分布如图 2.4 所示。

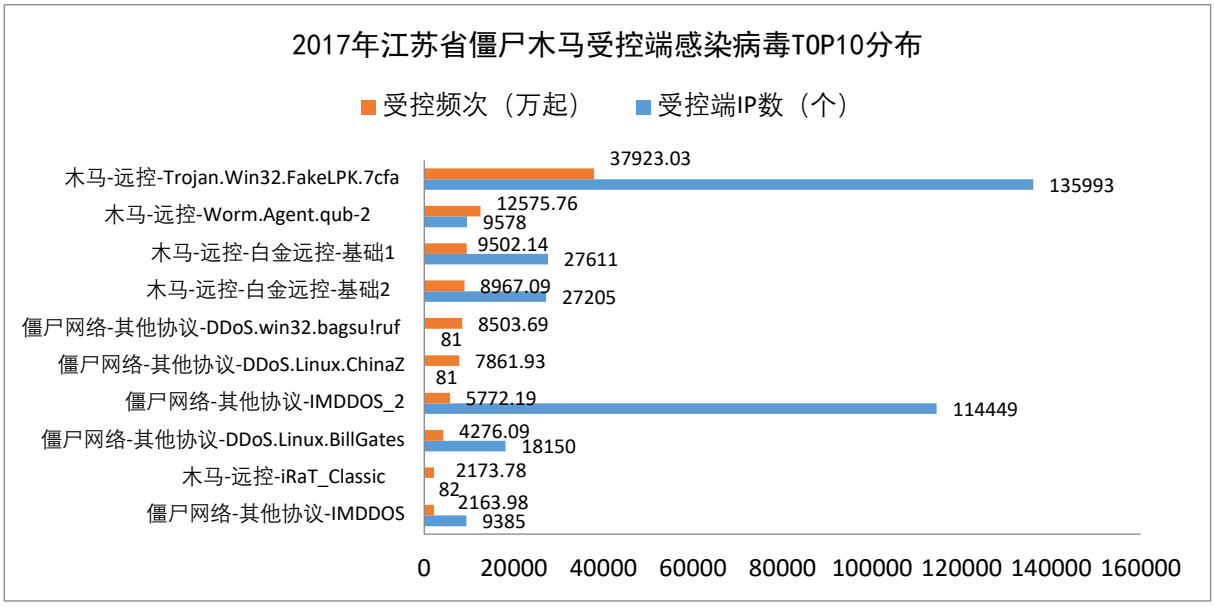
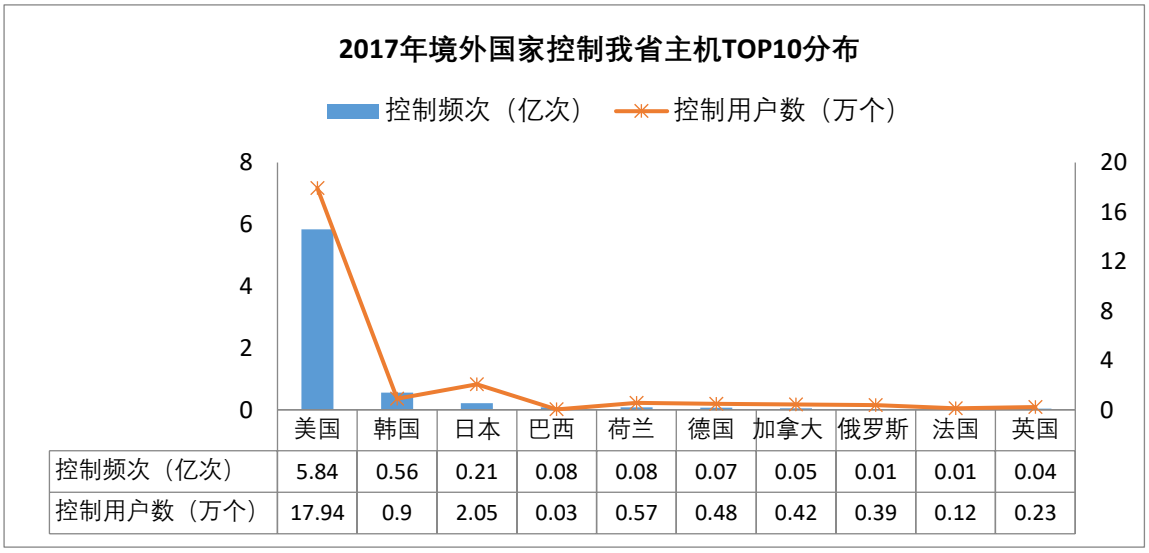


图 2.4 2017 年江苏省僵尸木马受控端感染病毒 TOP10 分布图

【TOP10 控制端国家分析】美国、韩国、日本等国家是境外控制江苏省主机数量最多的国家。其中，来自于美国的 1936 个 IP 地址控制了我省 17.94 万个 IP 地址，占总受控 IP 地址数的 29.04%，全年控制频次达 5.84 亿次；来自于韩国的 174 个 IP 地址控制了我省 9034 个 IP 地址，全年控制频次 5626.67 万次。境外国家控制我省主机分布如图 2.5 所示。



	美国	韩国	日本	巴西	荷兰	德国	加拿大	俄罗斯	法国	英国
控制频次（亿次）	5.84	0.56	0.21	0.08	0.08	0.07	0.05	0.01	0.01	0.04
控制用户数（万个）	17.94	0.9	2.05	0.03	0.57	0.48	0.42	0.39	0.12	0.23

图 2.5 2017 年境外国家控制我省主机 TOP10 分布图

【TOP10 受控 IP 地址分析】省内感染僵尸木马病毒成为受控主机，并与控制端通信的 TOP10 IP 地址中，与控制端通联频次最高的 IP 地址全年共通信 1911.46 万次。2017 年省内僵尸木马受控频次 TOP10 IP 地址情况如表 2.1 所示。

表 2.1 2017 年江苏省僵尸木马受控事件 TOP10 受控端 IP 地址表

排名	感染 IP 地址	事件次数	控制端国家	控制端数
1	219.xxx.xxx.41	19114620	美国	1
2	61.xxx.xxx.131	16360607	韩国、美国、日本	29
3	222.xxx.xxx.230	9498740	韩国、日本、美国	21
4	222.xxx.xxx.199	9451920	中国	1
5	125.xxx.xxx.164	8866260	韩国	1
6	211.xxx.xxx.194	8550024	韩国、日本	1
7	222.xxx.xxx. 235	8410699	巴西、美国、加拿大	59
8	218.xxx.xxx.77	6590760	中国	1
9	218.xxx.xxx.102	634270	美国	1
10	42.xxx.xxx.229	5295540	中国	1

2.2 僵尸木马控制端情况

2017 年，据江苏省互联网应急中心统计，我省利用僵尸木马对外控制的网络安全事件达 1.29 亿起，涉及 IP 地址 2647 个，控制端 IP 地址同比下降 19.96%。2013 至 2017 年江苏省僵尸木马控制事件总数分布如图 2.6 所示。2017 年江苏省僵尸木马控制事件数及控制端 IP 地址数月度分布如图 2.7 所示。

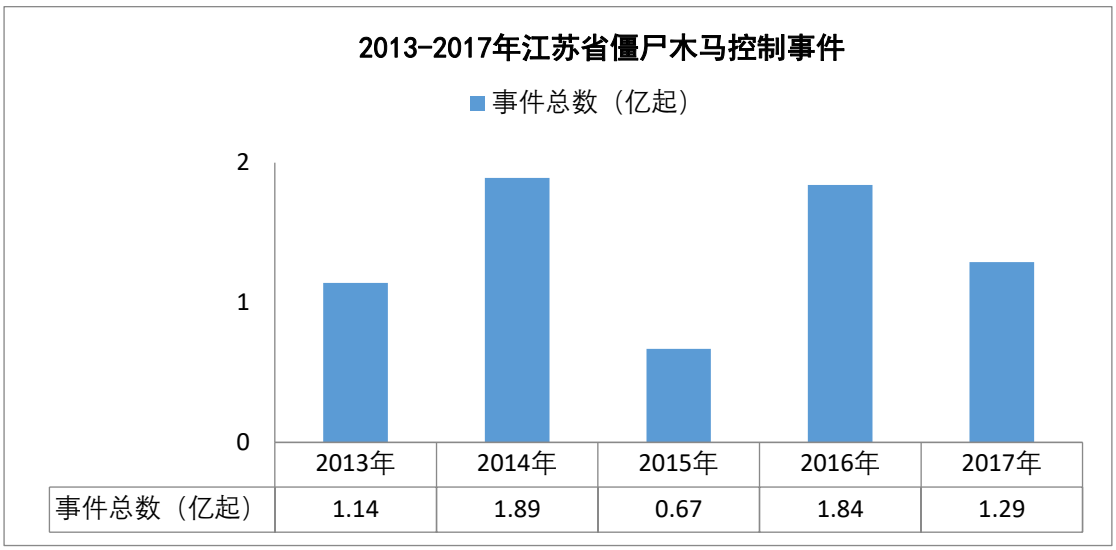
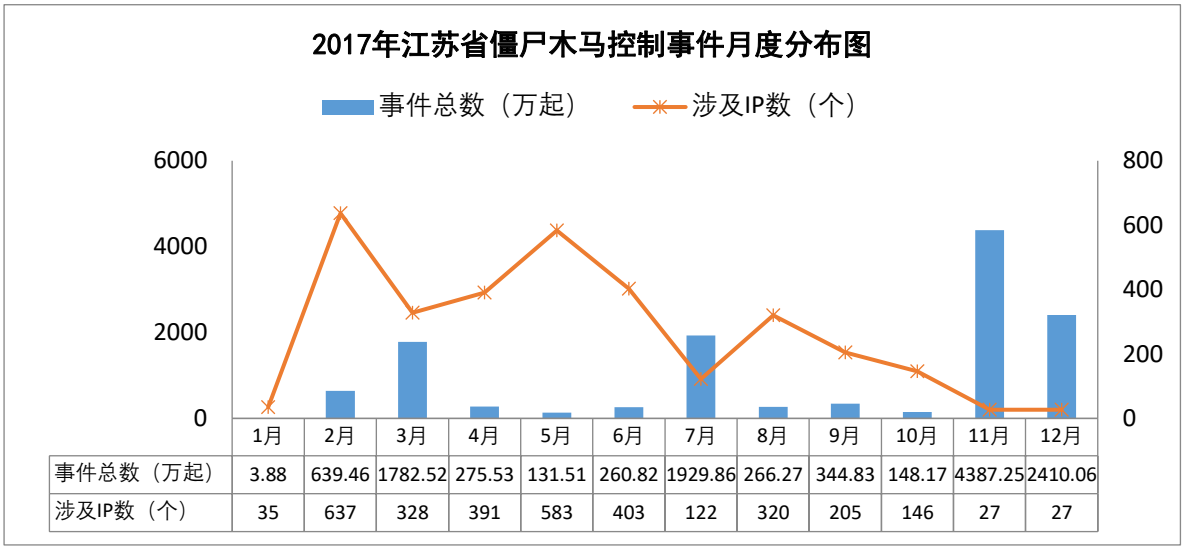


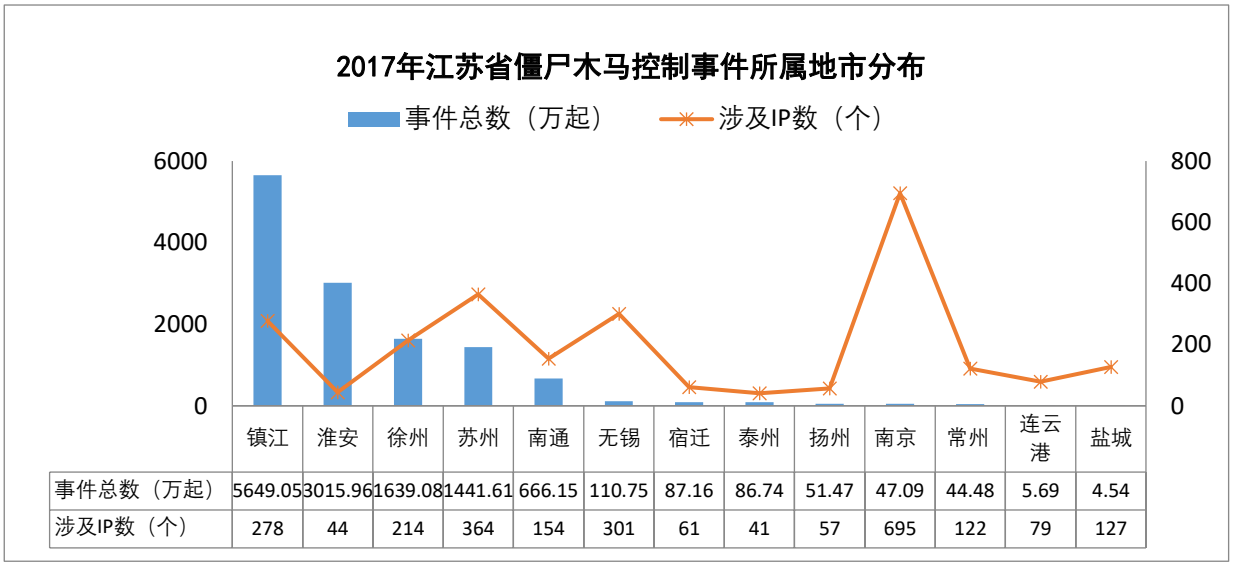
图 2.6 2013-2017 年江苏省僵尸木马控制事件总数分布图



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
事件总数（万起）	3.88	639.46	1782.52	275.53	131.51	260.82	1929.86	266.27	344.83	148.17	4387.25	2410.06
涉及IP数（个）	35	637	328	391	583	403	122	320	205	146	27	27

图 2.7 2017 年江苏省僵尸木马控制事件月度分布图

【控制事件所属设区市分布情况】2017 年，江苏省僵尸木马控制事件主要分布在镇江、淮安和徐州，其中镇江市发生僵尸木马控制事件最多，达到 5649.05 万起，涉及 IP 地址 278 个。2017 年江苏省僵尸木马控制事件所属设区市分布如图 2.8 所示。



	镇江	淮安	徐州	苏州	南通	无锡	宿迁	泰州	扬州	南京	常州	连云港	盐城
事件总数（万起）	5649.05	3015.96	1639.08	1441.61	666.15	110.75	87.16	86.74	51.47	47.09	44.48	5.69	4.54
涉及IP数（个）	278	44	214	364	154	301	61	41	57	695	122	79	127

图 2.8 2017 年江苏省僵尸木马控制事件所属设区市分布图

【控制端传播病毒类型 TOP10 分析】僵尸木马控制事件中，控制端主要通过 DDoS.Linux.ChinaZ、DDoS.win32.bagsu!ruf、木马-远控-白金远控-基础 2 等病毒传播，其中通过 DDoS.Linux.ChinaZ 木马控制的事件频次达 1.04 亿次，涉及 IP 地址 783 个。僵尸木马控制端传播病毒 TOP10 分布如图 2.9 所示。

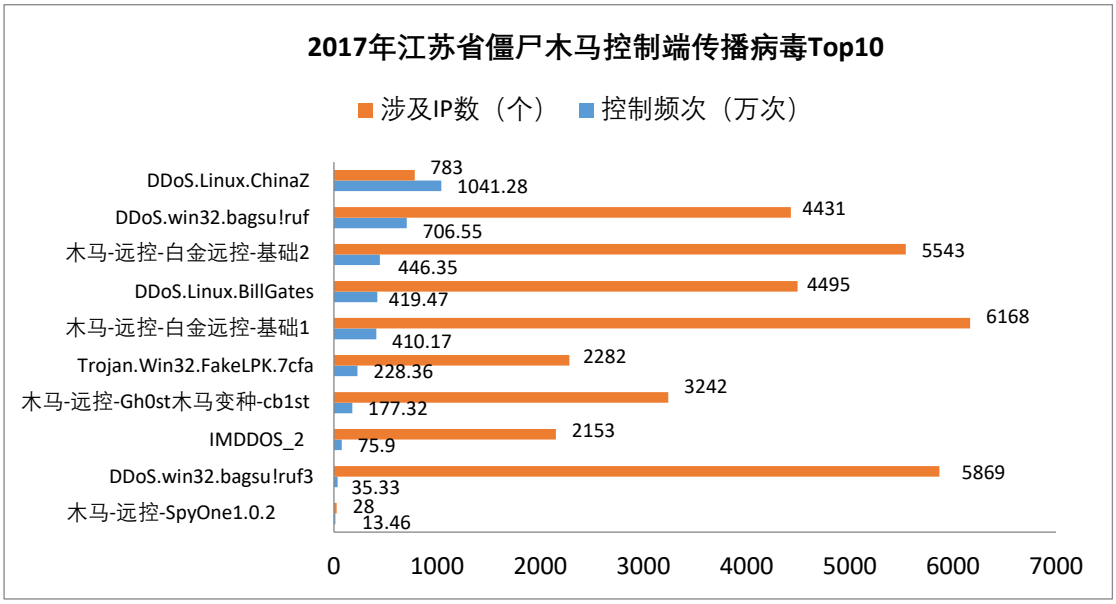


图 2.9 2017 年江苏省僵尸木马控制端传播病毒 TOP10 分布图

【TOP10 控制端 IP 地址分析】江苏省内僵尸木马控制服务器与受控端通信频次 TOP10 的 IP 地址中，事件发生次数最高的 IP 地址为 218.xxx.xx.113，实际控制的 IP 地址数 15 个，全年与受控端通信频次达 3015.08 万次。2017 年江苏省僵尸木马控制端事件 TOP10 IP 地址如表 2.2 所示。

表 2.2 2017 年江苏省僵尸木马控制事件 TOP10 控制端 IP 地址表

排名	TOP10 IP 地址	控制频次	控制 IP 数
1	218.xxx.xxx.113	30150830	15
2	222.xxx.xxx.38	17248668	102
3	58.xxx.xxx.72	14201261	14
4	222.xxx.xxx.86	11520616	15
5	180.xxx.xxx.98	7950836	35
6	222.xxx.xxx.151	5915808	148
7	222.xxx.xxx.136	5360551	27
8	180.xxx.xxx.139	3700521	40
9	58.xxx.xxx.152	3463415	4764
10	222.xxx.xxx.67	2889213	12

2.3 飞客蠕虫病毒感染情况

2017 年，据江苏省互联网应急中心监测统计，省内感染飞客蠕虫病毒事件达 554.36 万起，涉及 25.57 万个 IP 地址，同比下降 44.98%。2013 至 2017 年感

染飞客蠕虫病毒事件数分布如图 2.10 所示。2017 年飞客蠕虫病毒感染月度分布如图 2.11 所示。

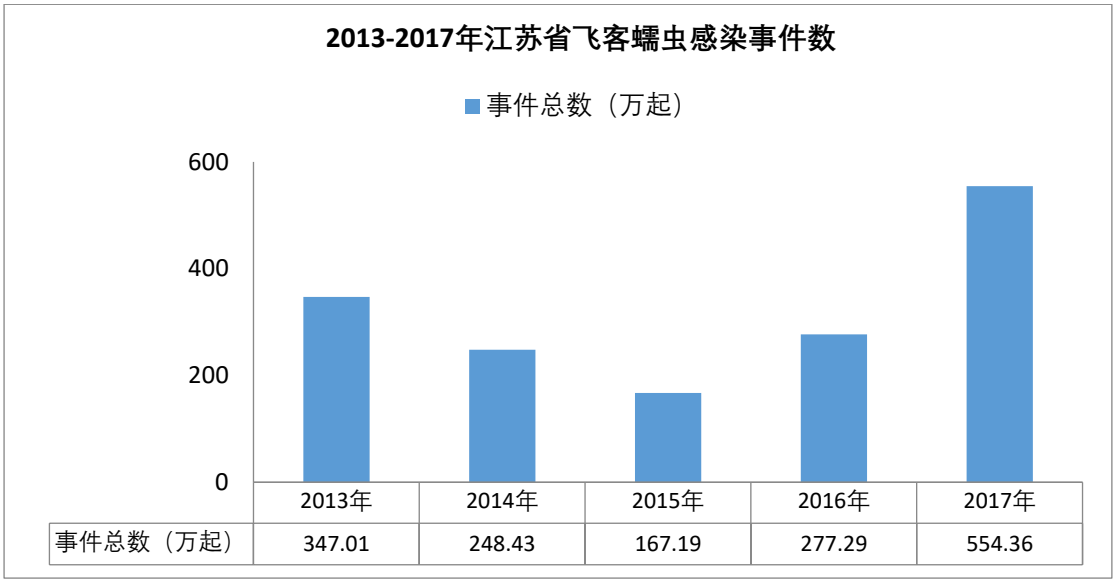


图 2.10 2013-2017 年江苏省飞客蠕虫病毒感染事件总数分布图

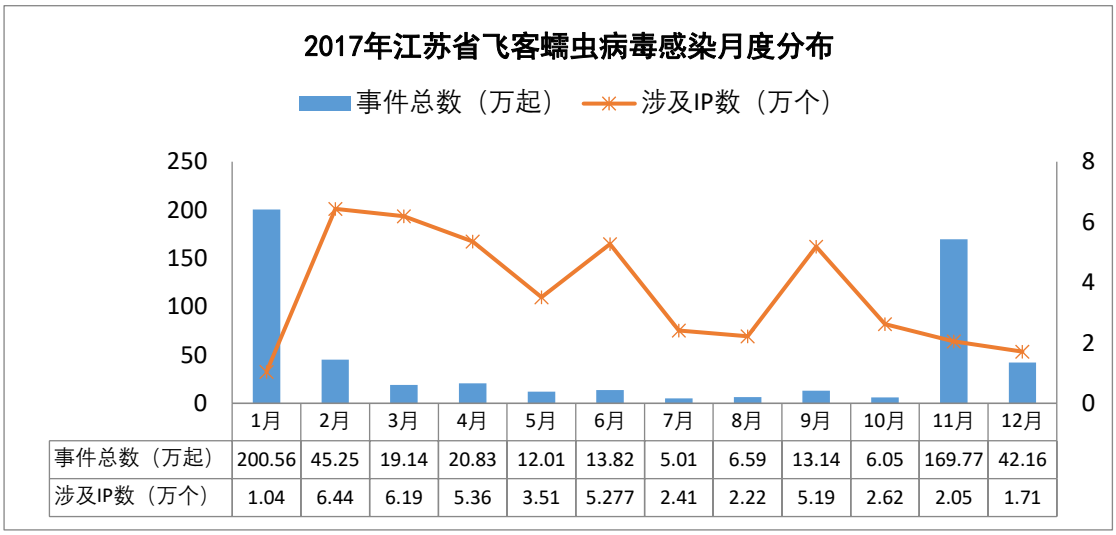
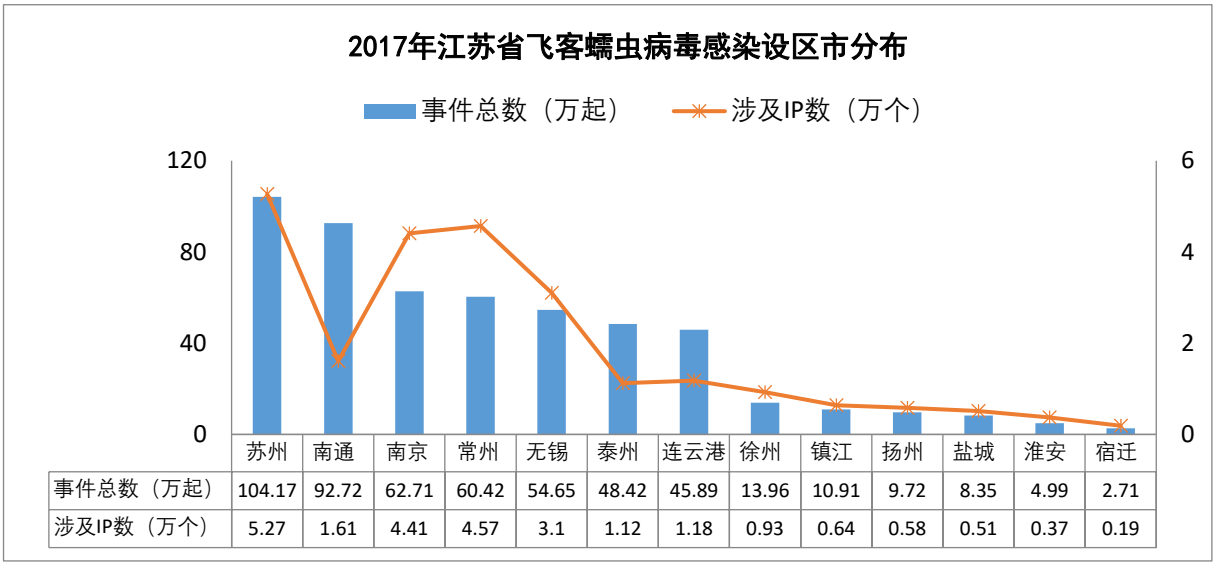


图 2.11 2017 江苏省飞客蠕虫病毒感染月度分布图

【感染飞客蠕虫事件数所属设区市分析】2017 年，我省感染飞客蠕虫病毒的主机主要分布在苏州、常州和南京，其中苏州 5.27 万个 IP 地址感染飞客蠕虫病毒，事件总数达 104.17 万起，2017 年飞客蠕虫病毒感染所属设区市分布如图 2.12 所示。



	苏州	南通	南京	常州	无锡	泰州	连云港	徐州	镇江	扬州	盐城	淮安	宿迁
事件总数（万起）	104.17	92.72	62.71	60.42	54.65	48.42	45.89	13.96	10.91	9.72	8.35	4.99	2.71
涉及IP数（万个）	5.27	1.61	4.41	4.57	3.1	1.12	1.18	0.93	0.64	0.58	0.51	0.37	0.19

图 2.12 2017 年江苏省飞客蠕虫病毒感染所属设区市分布图

【感染 IP 地址 TOP10 分析】江苏省感染飞客蠕虫病毒的主机中，通信频次最高的全年共通信 12.41 万次。2017 年，感染飞客蠕虫病毒通信频次 TOP10 的 IP 地址分布如表 2.3 所示。

表 2.3 2017 年江苏省感染飞客蠕虫病毒事件 TOP10 IP 地址表

排名	飞客病毒类型	感染 IP	通信频次
1	conficker.b	211.xxx.xxx.195	124140
2	conficker.b	122.xxx.xxx.34	9659
3	conficker.b	211.xxx.xxx.210	7118
4	conficker.b	211.xxx.xxx.234	7010
5	conficker.b	221.xxx.xxx.54	6837
6	conficker.b	221.xxx.xxx.82	5881
7	conficker.b	218.xxx.xxx.150	5842
8	conficker.b	121.xxx.xxx.142	5175
9	conficker.b	211.xxx.xxx.130	4806
10	conficker.b	211.xxx.xxx.186	4748

3、移动互联网恶意程序感染情况

3.1 移动互联网恶意程序传播和活动情况

随着智能终端普及，越来越多的移动互联网恶意程序随之出现。2010 年至 2017 年 CNCERT/CC 通过监测和厂商交换获得恶意程序数量逐年增多，2017 年共发现移动互联网恶意程序 253.33 万个，同比增长 23.36%。2010 年至 2017 年移动互联网恶意程序数量分布如图 3.1 所示。按行为属性统计，2017 年移动互联网恶意程序程序中“流氓行为”属性所占比例最高，数量达 91.00 万个，占总数的 35.92%。2017 年移动互联网恶意程序数量按危害等级统计如图 3.2 所示。

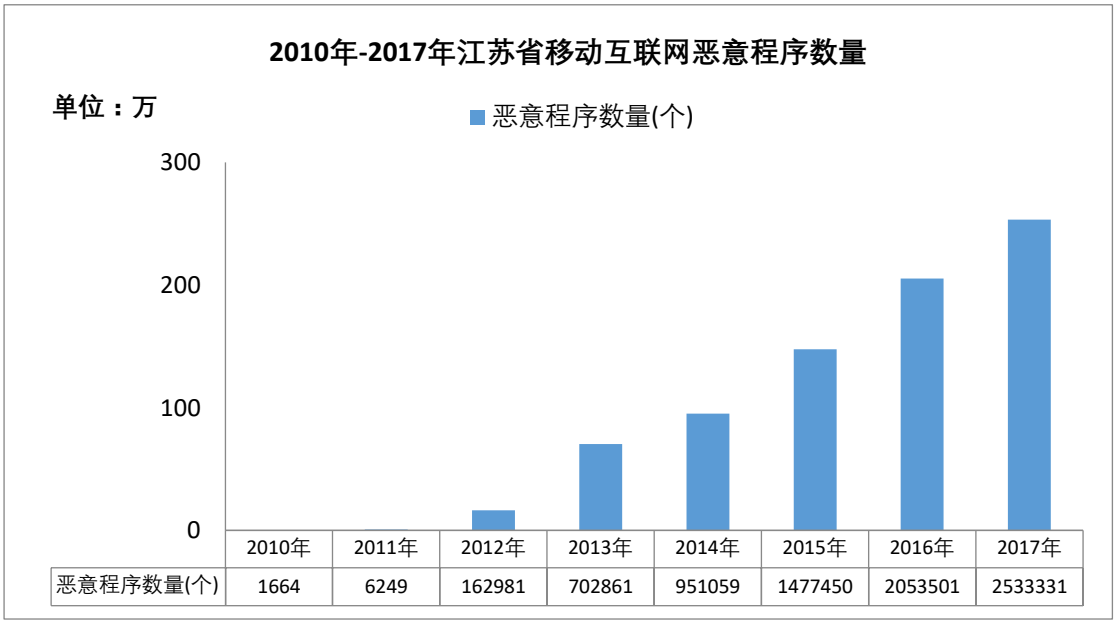


图 3.1 2010-2017 年江苏省移动互联网恶意程序数量分布图

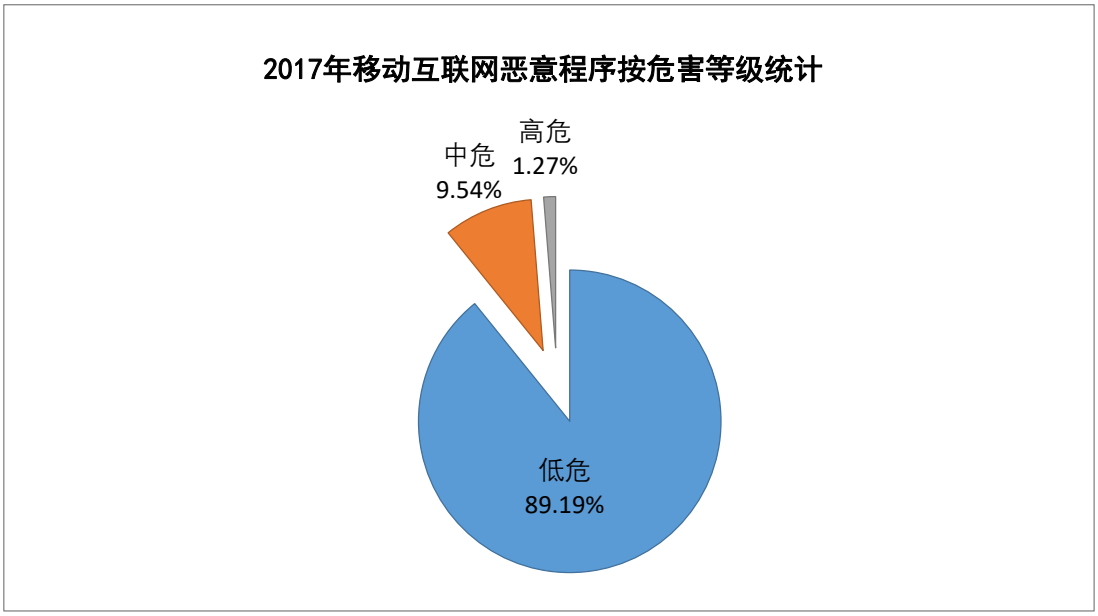
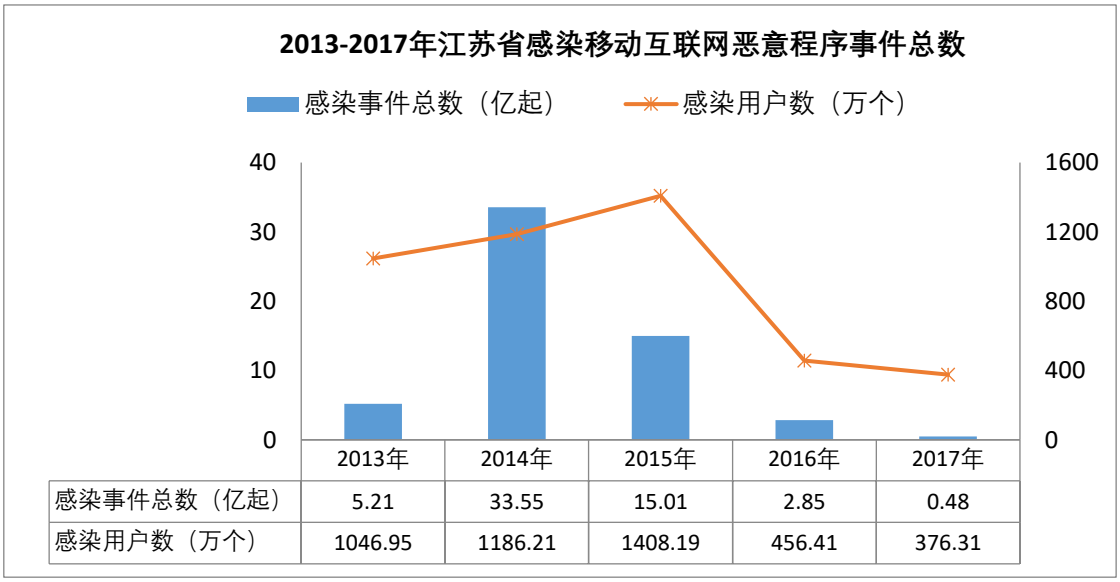


图 3.2 2017 年移动互联网恶意程序按危害等级统计图

3.2 移动互联网恶意程序感染情况

2017 年，江苏省互联网应急中心发现全省各类移动互联网恶意程序感染事件 4779.64 万起，平均每月有 31.36 万个用户感染。2013 至 2017 年江苏省移动互联网恶意程序感染事件总数分布如图 3.3 所示。



	2013年	2014年	2015年	2016年	2017年
感染事件总数（亿起）	5.21	33.55	15.01	2.85	0.48
感染用户数（万个）	1046.95	1186.21	1408.19	456.41	376.31

图 3.3 2013-2017 年江苏省感染移动互联网恶意程序事件总数分布图

3.3 移动互联网恶意程序行为属性

根据通信行业标准 YD/T 2439-2012《移动互联网恶意程序描述格式》的规定，移动互联网恶意程序主要分为恶意扣费、流氓行为、诱骗欺诈、隐私窃取、资费消耗、系统破坏、恶意传播、远程控制等类型。其中，恶意扣费、隐私窃取和远程控制的危害级别最高。2017 年移动互联网恶意程序按行为属性统计如图 3.4 所示.2017 年，江苏省互联网应急中心发现我省感染用户数最多的恶意程序类型为恶意扣费类。2017 年江苏省移动互联网恶意程序类型分布事件数如图 3.5 所示。

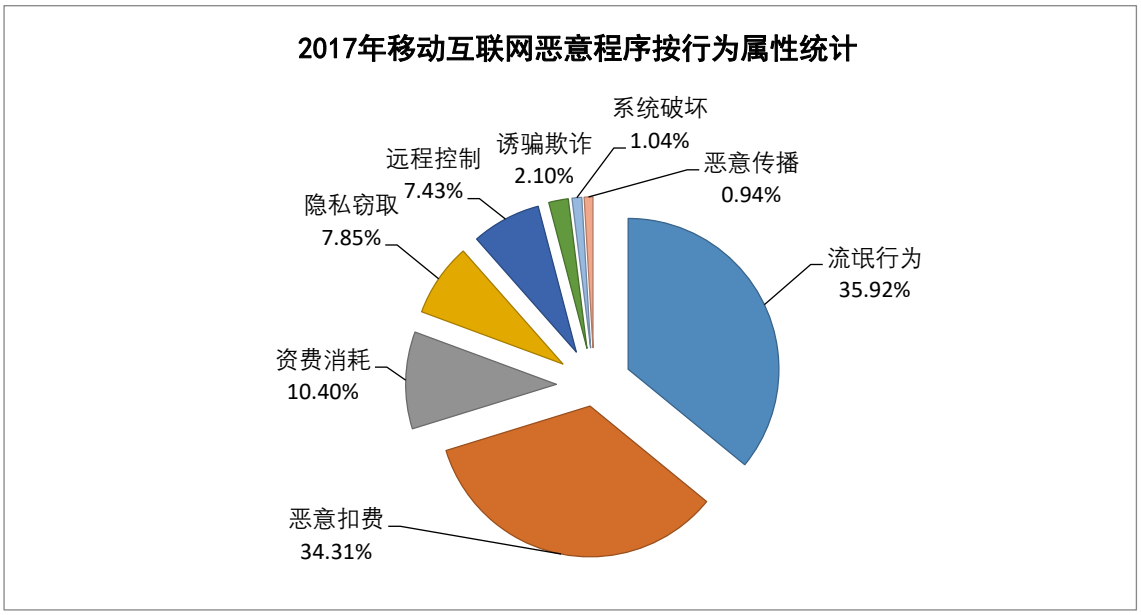
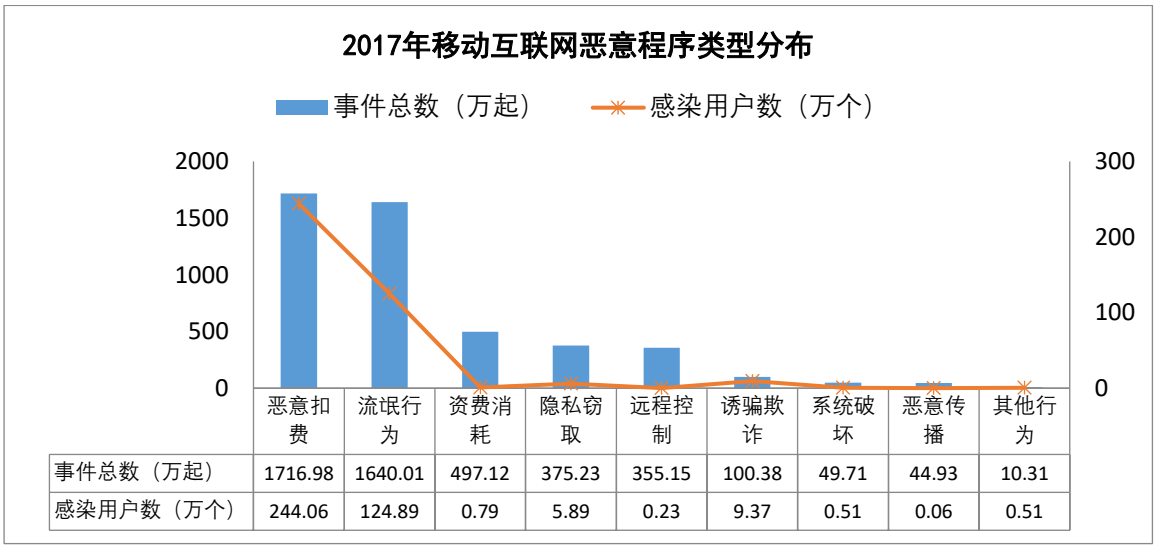


图 3.4 2017 年移动互联网恶意程序按行为属性统计图

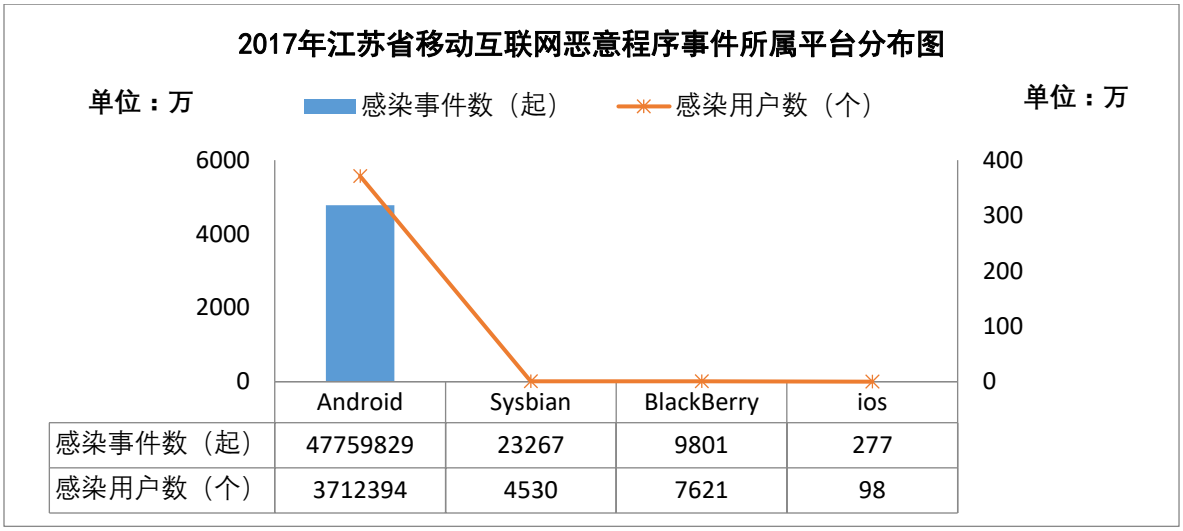


	恶意扣费	流氓行为	资费消耗	隐私窃取	远程控制	诱骗欺诈	系统破坏	恶意传播	其他行为
事件总数（万起）	1716.98	1640.01	497.12	375.23	355.15	100.38	49.71	44.93	10.31
感染用户数（万个）	244.06	124.89	0.79	5.89	0.23	9.37	0.51	0.06	0.51

图 3.5 2017 年江苏省移动互联网恶意程序事件类型分布图

3.4 移动互联网恶意程序感染平台分析

2017 年，江苏省互联网应急中心发现 Android 平台是用户感染恶意程序最多的手机操作系统。其中 Android 平台感染用户数最多，全年共有 371.24 万个用户感染，BlackBerry 平台全年共有 7621 个用户感染，Sysbian 平台全年共有 4530 个用户感染。2017 年江苏省移动互联网恶意程序感染事件所属平台分布如图 3.6 所示。

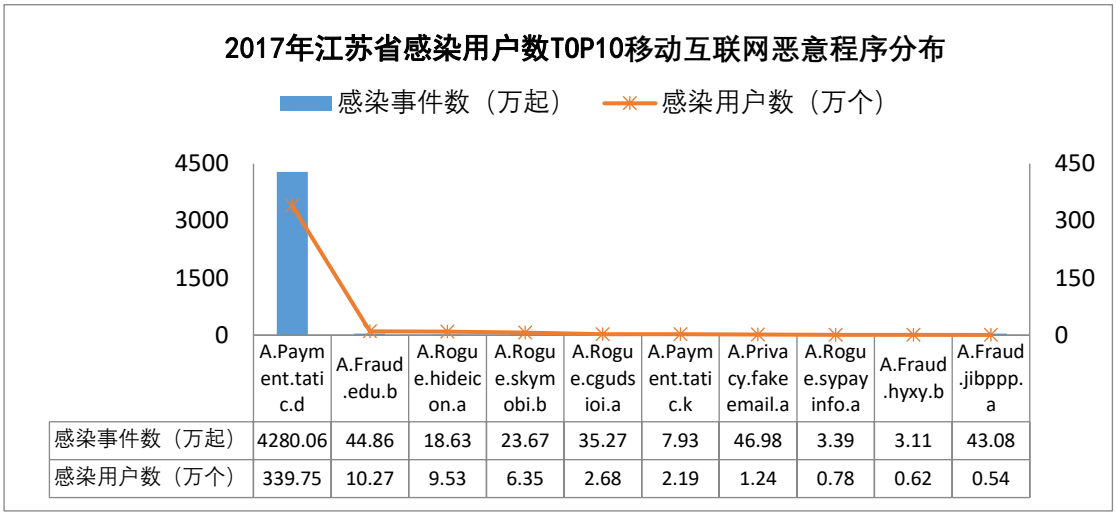


	Android	Sysbian	BlackBerry	ios
感染事件数（起）	47759829	23267	9801	277
感染用户数（个）	3712394	4530	7621	98

图 3.6 2017 年江苏省移动互联网恶意程序事件所属平台分布图

3.5 移动互联网恶意程序感染用户 TOP10

2017 年，江苏省移动互联网恶意程序感染用户数较多的三种病毒分别为 A.Payment.tatic.d、A.Fraud.edu.b、A.Rogue.hideicon.a 病毒。A.Payment.tatic.d 病毒的主要行为是私自发送订购短信到指定号码，在用户不知情的情况下下载未知应用，私自拦截用户短信，并创建色情类应用快捷方式，该病毒存在恶意扣费、资费消耗、流氓行为等属性。A.Fraud.edu.b 病毒主要是诱导用户开通观影会员，实质上开通会员后并不能观看视频内容，且其中包含大量不良信息，属于诱骗欺诈、流氓行为。A.Rogue.hideicon.a 病毒包含广告插件，安装后无图标且存在私自下载的风险行为。感染用户数 TOP10 病毒感染情况如图 3.7 所示。



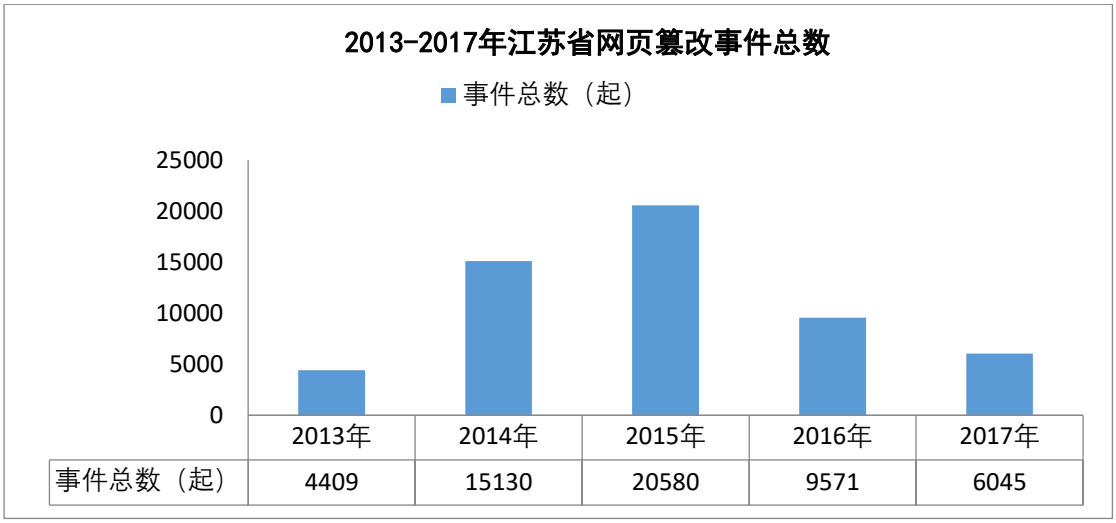
	A.Payment.tatic.d	A.Fraud.edu.b	A.Rogue.hideicon.a	A.Rogue.skymobi.b	A.Rogue.cgudsioi.a	A.Payment.tatic.k	A.Privacy.fakeemail.a	A.Rogue.sypayinfo.a	A.Fraud.hyxy.b	A.Fraud.jibppp.a
感染事件数（万起）	4280.06	44.86	18.63	23.67	35.27	7.93	46.98	3.39	3.11	43.08
感染用户数（万个）	339.75	10.27	9.53	6.35	2.68	2.19	1.24	0.78	0.62	0.54

图 3.7 2017 年江苏省感染用户数 TOP10 移动互联网恶意程序分布图

4、网站安全监测情况

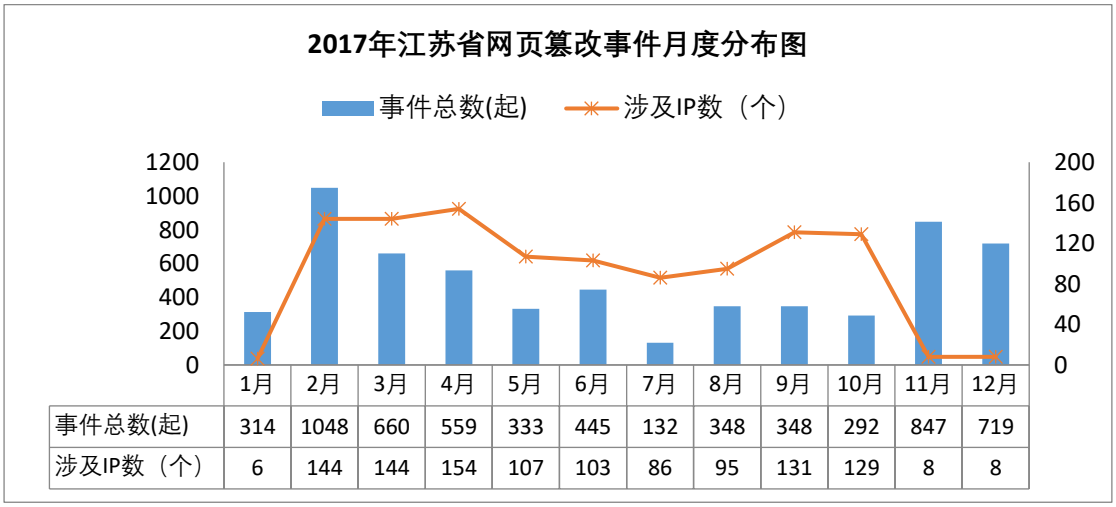
4.1 网页篡改事件

2017 年，据江苏省互联网应急中心统计，江苏省共发生 6045 起网页篡改事件，同比下降 36.84%，其中 2 月份发生的网页篡改事件数最多，占总事件数的 17.33%。2013 年至 2017 年江苏省网页篡改事件总数分布如图 4.1 所示，2017 年江苏省网页篡改事件总数月度分布如图 4.2 所示。



	2013年	2014年	2015年	2016年	2017年
事件总数（起）	4409	15130	20580	9571	6045

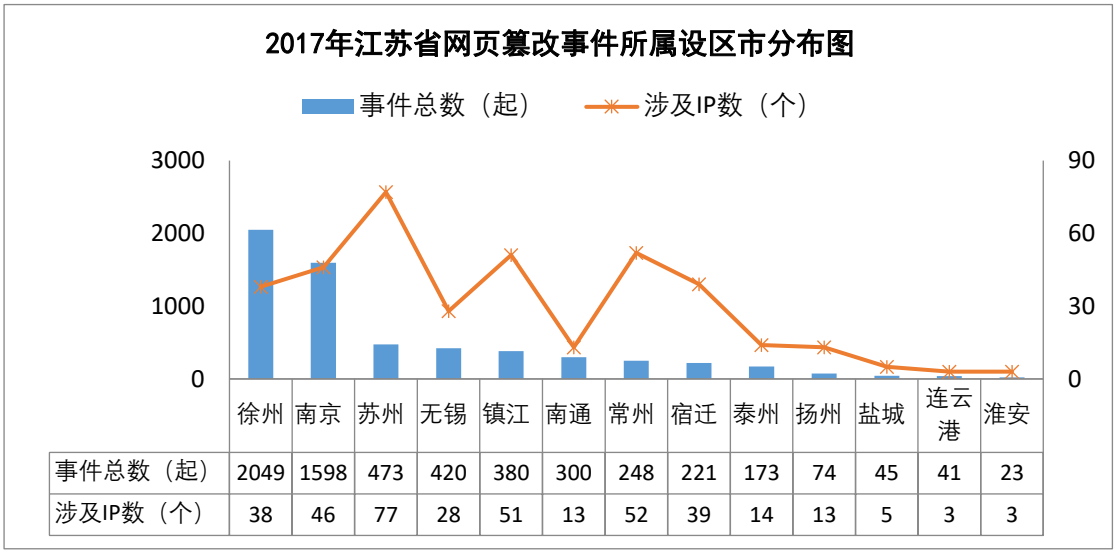
图 4.1 2013-2017 年江苏省网页篡改事件总数分布图



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
事件总数(起)	314	1048	660	559	333	445	132	348	348	292	847	719
涉及IP数（个）	6	144	144	154	107	103	86	95	131	129	8	8

图 4.2 2017 年江苏省网页篡改事件总数月度分布图

【网页篡改事件所属设区市分布情况】2017 年，江苏省发生网页篡改事件较多的设区市为徐州、南京和苏州，其中徐州发生 2049 起，南京发生 1598 起，苏州发生 473 起，2017 年江苏省网页篡改事件所属设区市分布如图 4.3 所示。



	徐州	南京	苏州	无锡	镇江	南通	常州	宿迁	泰州	扬州	盐城	连云港	淮安
事件总数（起）	2049	1598	473	420	380	300	248	221	173	74	45	41	23
涉及IP数（个）	38	46	77	28	51	13	52	39	14	13	5	3	3

图 4.3 2017 年江苏省网页篡改事件所属设区市分布图

【攻击动因分析】按照攻击手段，网页篡改可以分成显式篡改和隐式篡改两种。通过显式篡改，黑客可炫耀自己的技术技巧，或达到声明自己主张的目的；隐式篡改一般是在被攻击网站的网页中植入含有色情、诈骗等非法信息的暗链，以助黑客谋取非法经济利益。黑客为了篡改网页，一般需提前知晓网站的漏洞，在网页中植入后门，并最终获取网站的控制权。

● **赌博广告类网页篡改事件截图：**

图 4.4 某市审计局网站遭受赌博类篡改截图

图 4.5 广告类篡改网页截图

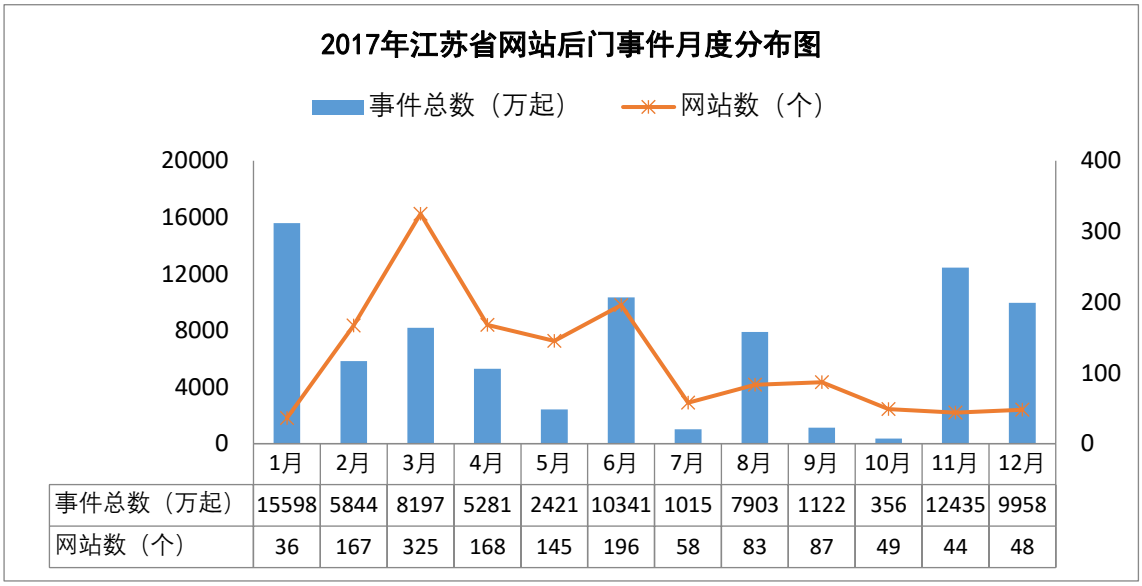
● **网站黑页类型篡改截图：**

图 4.6 网站黑页类型篡改截图

4.2 网站后门[1]事件

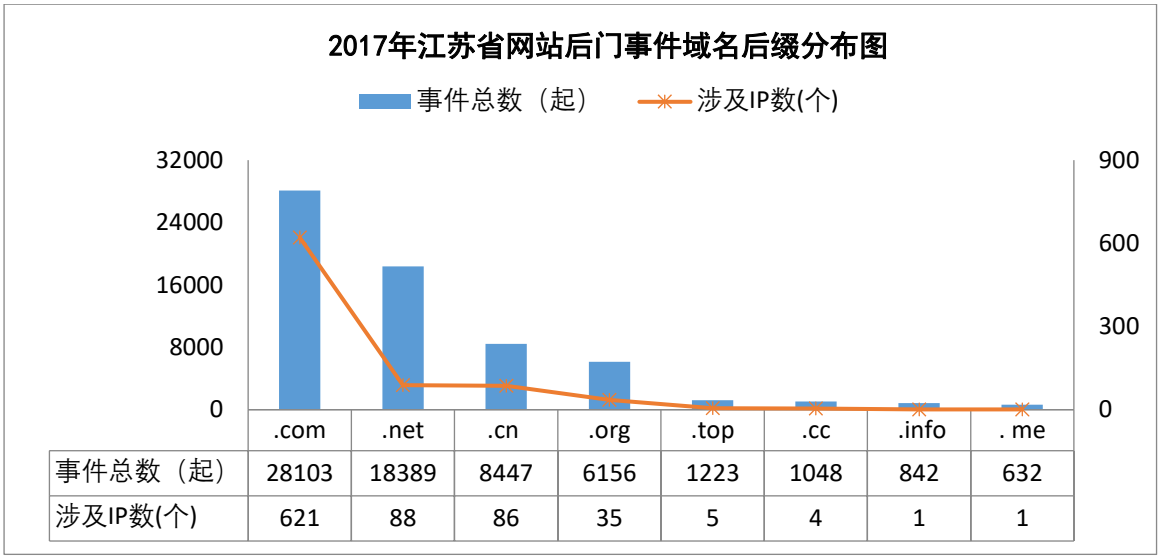
2017 年，据江苏省互联网应急中心统计，江苏省共发生 8.05 万起网站后门事件，共计 1163 个网站被植入后门。其中，1 月份发生的网站后门事件数最多，占总事件数的 19.38%。被植入后门的网站中，.com 后缀域名网站 621 个，.net 后缀域名网站 88 个，.cn 后缀域名网站 86 个。2017 年江苏省被植入网站后门事件月度分布图和所属域名分布图如图 4.7、4.8 所示。

[1]网站后门，指黑客利用网站漏洞上传到网站源代码中的脚本文件，利用脚本文件长期控制网站，如进行网站文件操作、服务器提权、数据库操作等。



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
事件总数（万起）	15598	5844	8197	5281	2421	10341	1015	7903	1122	356	12435	9958
网站数（个）	36	167	325	168	145	196	58	83	87	49	44	48

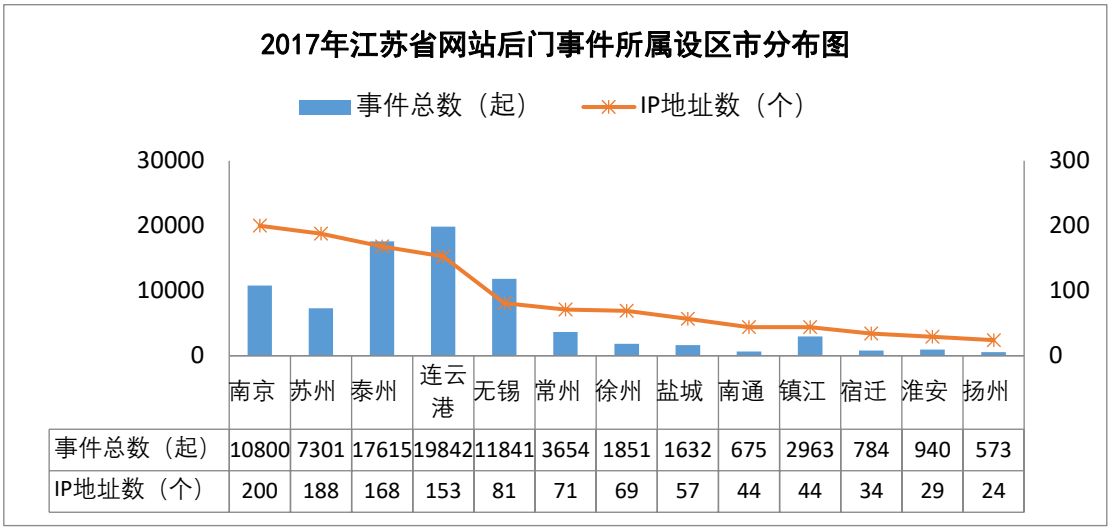
图 4.7 2017 年江苏省网站后门事件月度分布图



	.com	.net	.cn	.org	.top	.cc	.info	. me
事件总数（起）	28103	18389	8447	6156	1223	1048	842	632
涉及IP数(个)	621	88	86	35	5	4	1	1

图 4.8 2017 年江苏省网站后门事件域名后缀分布图

【网站后门事件所属设区市分布情况】2017 年，江苏省网站被植入后门较多的设区市为南京、苏州、泰州，其中南京发生后门事件 1.08 万起，涉及网站 280 个，苏州发生 7301 起，涉及网站 263 个，泰州发生 1.76 万起，涉及网站 236 个，2017 年江苏省网站后门事件所属设区市分布和网站后门事件截图分别如图 4.9、4.10 所示。



	南京	苏州	泰州	连云港	无锡	常州	徐州	盐城	南通	镇江	宿迁	淮安	扬州
事件总数（起）	10800	7301	17615	19842	11841	3654	1851	1632	675	2963	784	940	573
IP地址数（个）	200	188	168	153	81	71	69	57	44	44	34	29	24

图 4.9 江苏省网站后门事件所属设区市分布图

● **网站后门事件截图：**

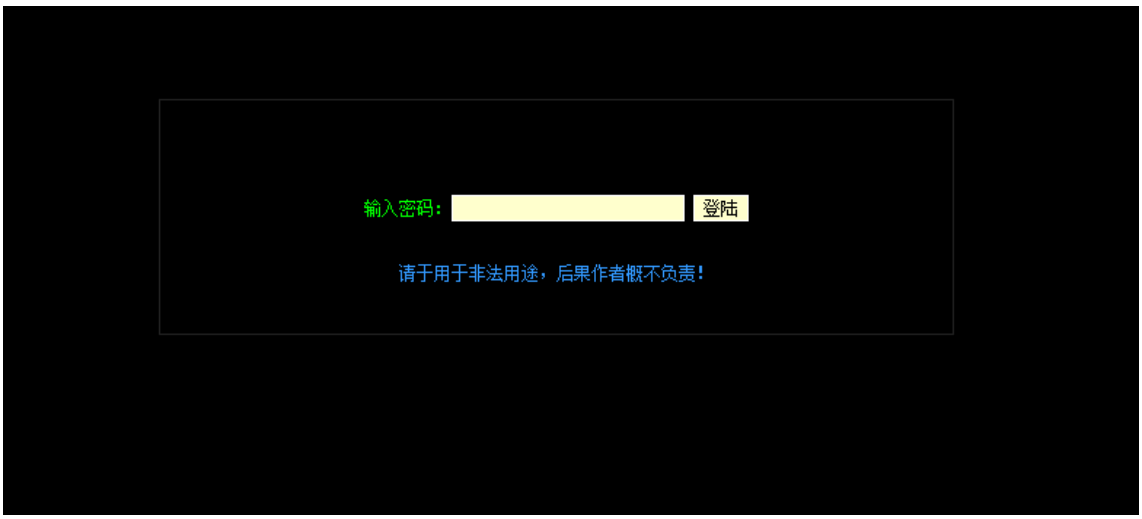


图 4.10 网站后门事件截图

4.3 网页仿冒事件

据江苏省互联网应急中心统计，2017 年，江苏省发生网页仿冒事件 9013 起，同比减少 26.12%。其中，4 月份发生的网页仿冒事件数最多，占总事件数的 15.68%。2013 至 2017 年江苏省网页仿冒事件总数分布和 2017 年江苏省网页仿冒事件月度分布，分别如图 4.11 和 4.12 所示。

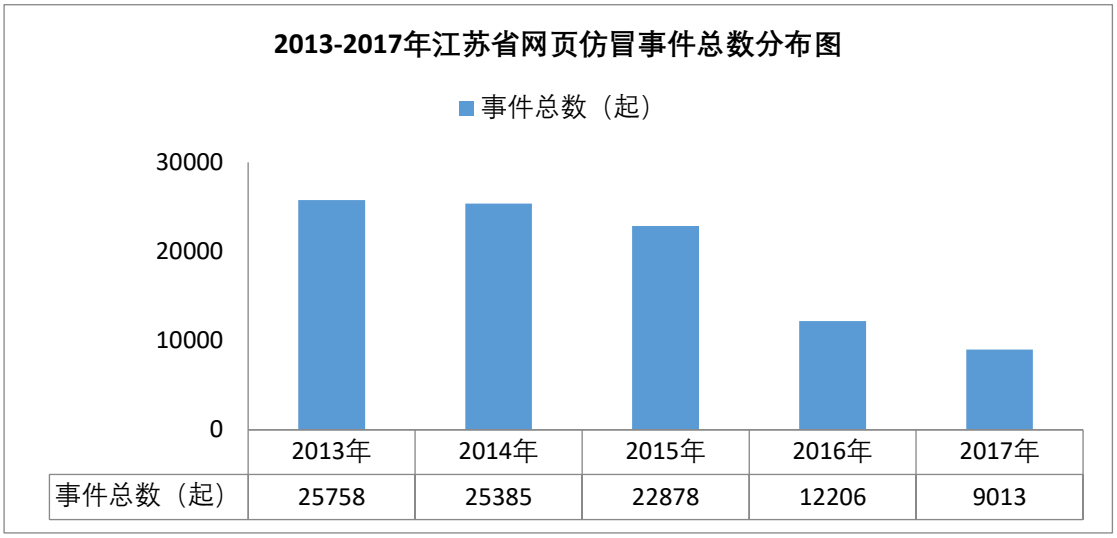


图 4.11 2013-2017 年江苏省网页仿冒事件总数分布图

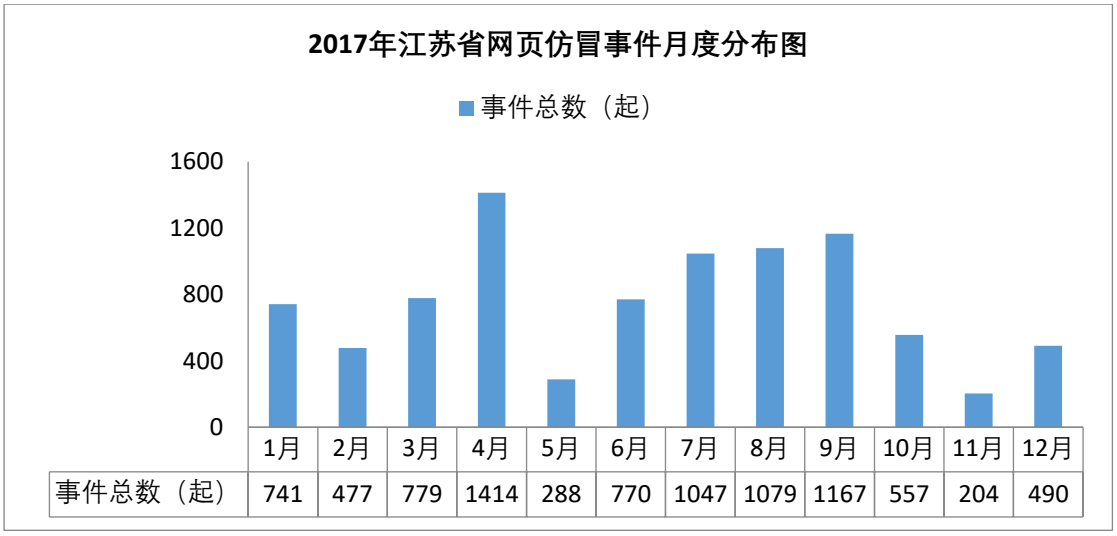


图 4.12 2017 年江苏省网页仿冒事件月度分布图

【事件类型分布情况】网页仿冒事件中，“虚假购物[2]”类型的仿冒事件最多，达到 3898 起，占总数的 43.25%；其次，“虚假招聘”类型的仿冒事件 2333 起，占总数的 25.88%。2017 年江苏省仿冒事件所属类型占比分布如图 4.13 所示。

[2]虚假购物主要指假淘宝、假手机充值等涉及购物欺诈的钓鱼网站。

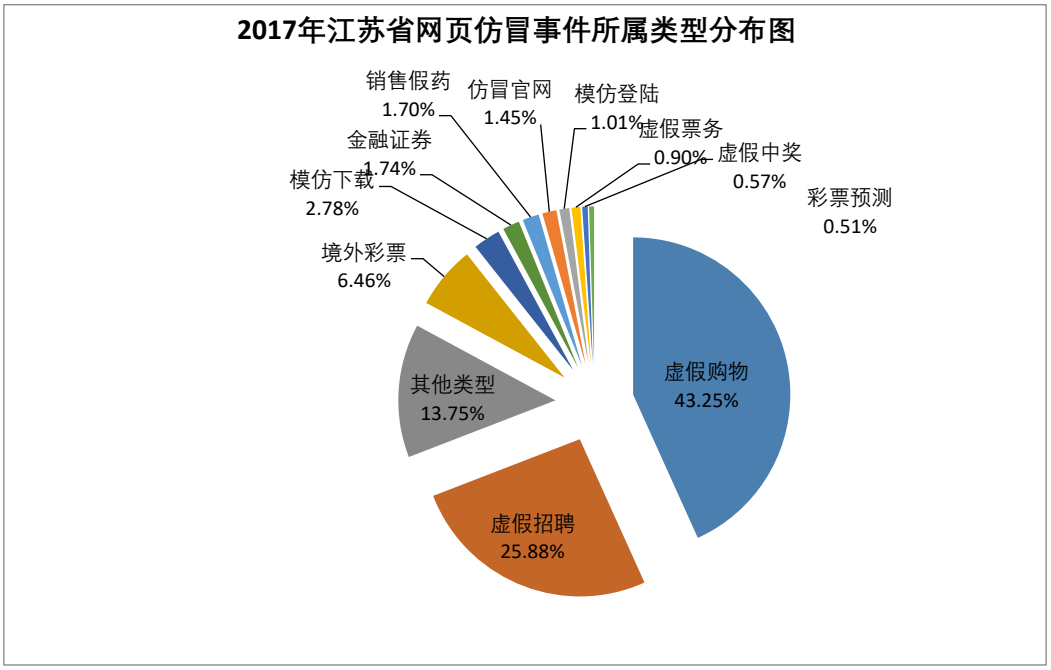
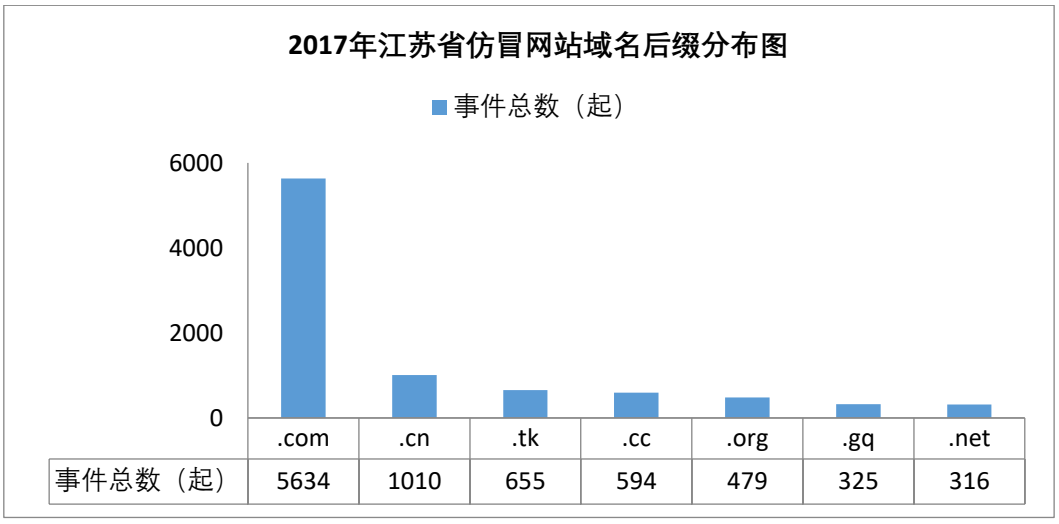


图 4.13 2017 年江苏省网页仿冒事件所属类型分布图

【仿冒网站注册域名类型分布情况】仿冒网站的主要域名类型包括.com、.cn 和.tk 等，其中.com 是注册仿冒网站最多的域名类型。2017 年江苏省仿冒网站域名后缀分布如图 4.14 所示，仿冒中国工商银行网站事件如图 4.15 所示。



	.com	.cn	.tk	.cc	.org	.gq	.net
事件总数（起）	5634	1010	655	594	479	325	316

图 4.14 2017 年江苏省仿冒网站域名后缀分布图

图 4.15 仿冒中国工商银行网站事件截图

4.4 网页挂马事件

2017 年，据江苏省互联网应急中心统计，江苏省发生网页挂马事件 8.19 万起，放马源网站 172 个。其中，4 月份发生的网页挂马事件数最多，占总事件数的 71.12%。2013 至 2017 年江苏省网页挂马事件总数分布和 2017 年网页挂马事件月度分布，分别如图 4.16 和图 4.17 所示。

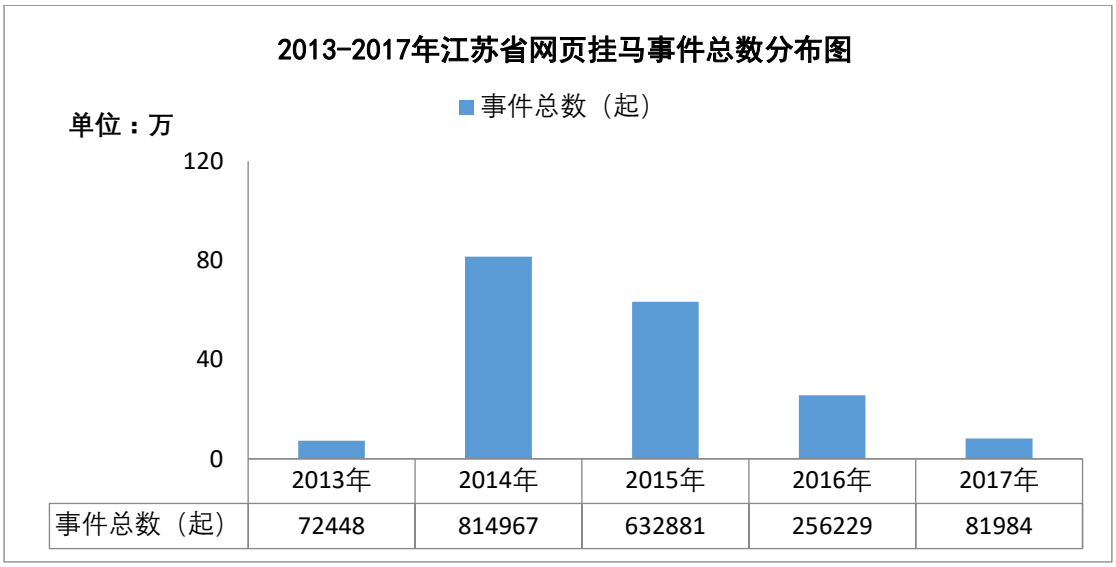
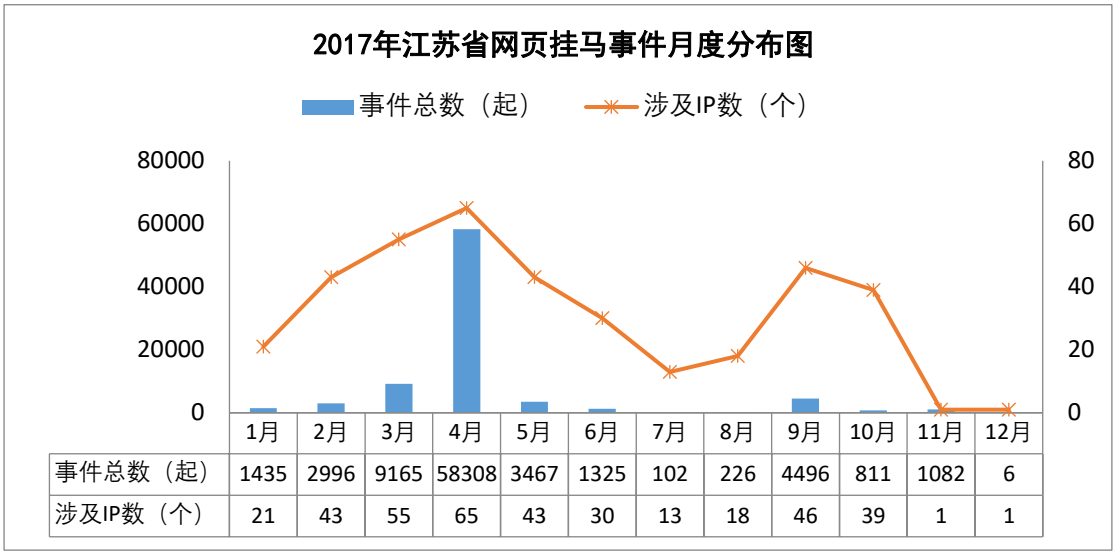


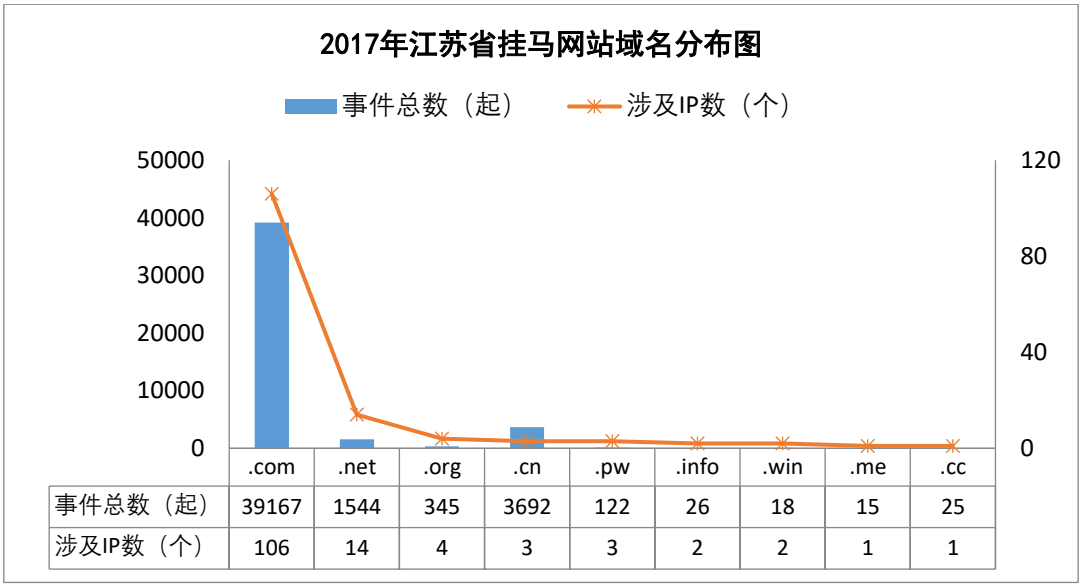
图 4.16 2013-2017 年江苏省网页挂马事件总数分布图



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
事件总数（起）	1435	2996	9165	58308	3467	1325	102	226	4496	811	1082	6
涉及IP数（个）	21	43	55	65	43	30	13	18	46	39	1	1

图 4.17 2017 年江苏省网页挂马事件月度分布图

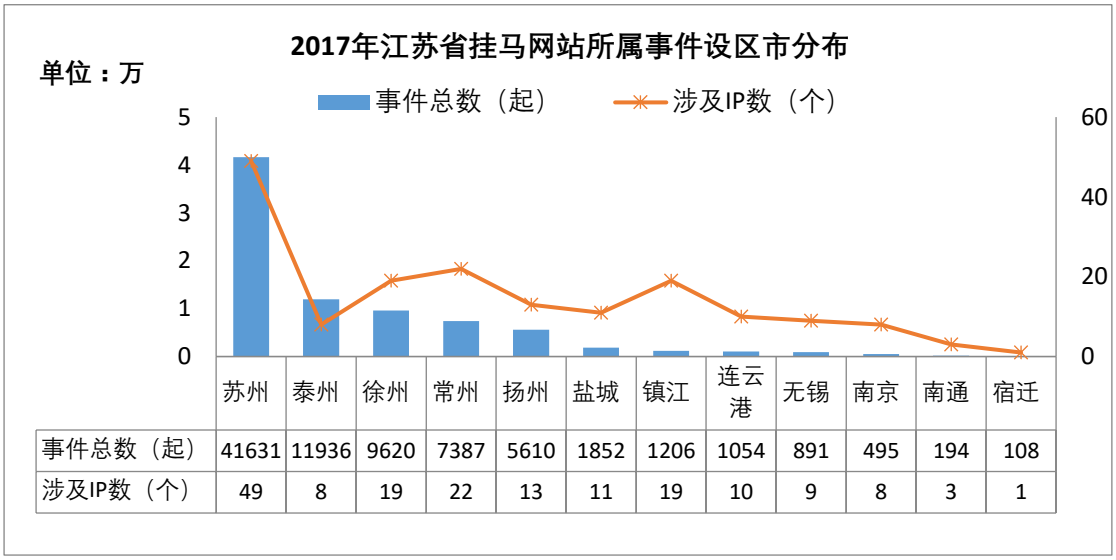
【挂马网站域名后缀分布情况】2017 年网页挂马事件中被挂马的网站域名后缀包括.com、.net、.org、.cn、.pw、.info、.win 等，其中.com、.cn 和.net 是遭受挂马最多的域名，挂马事件数分别为 3.91 万起、3692 起、1544 起，挂马网站事件域名分布如图 4.18 所示。



	.com	.net	.org	.cn	.pw	.info	.win	.me	.cc
事件总数（起）	39167	1544	345	3692	122	26	18	15	25
涉及IP数（个）	106	14	4	3	3	2	2	1	1

图 4.18 2017 年江苏省网页挂马网站域名分布图

【挂马网站所属设区市分布情况】2017 年，江苏省发生网页挂马事件较多的设区市为苏州、泰州和徐州，其中苏州发生 4.16 万起，泰州发生 1.19 万起，徐州发生 9620 起，2017 年江苏省挂马网站所属设区市分布如图 4.19 所示。



	苏州	泰州	徐州	常州	扬州	盐城	镇江	连云港	无锡	南京	南通	宿迁
事件总数（起）	41631	11936	9620	7387	5610	1852	1206	1054	891	495	194	108
涉及IP数（个）	49	8	19	22	13	11	19	10	9	8	3	1

图 4.19 2017 年江苏省挂马网站所属设区市分布图

【网页放马源分析】一些网站作为放马服务器的形式出现，这些网站往往被黑客或挂马集团掌控，或用作恶意跳转链接，或作为恶意代码下载服务器。特别是动态域名，许多可以在国内外多家域名注册商注册，且注册成本相对较为低廉。实施网页挂马的黑客或挂马集团往往会批量注册，在一段时间内不断变换使用，以隐藏自己的活动痕迹，规避监管，增加治理的难度。

● **网页挂马事件截图：**

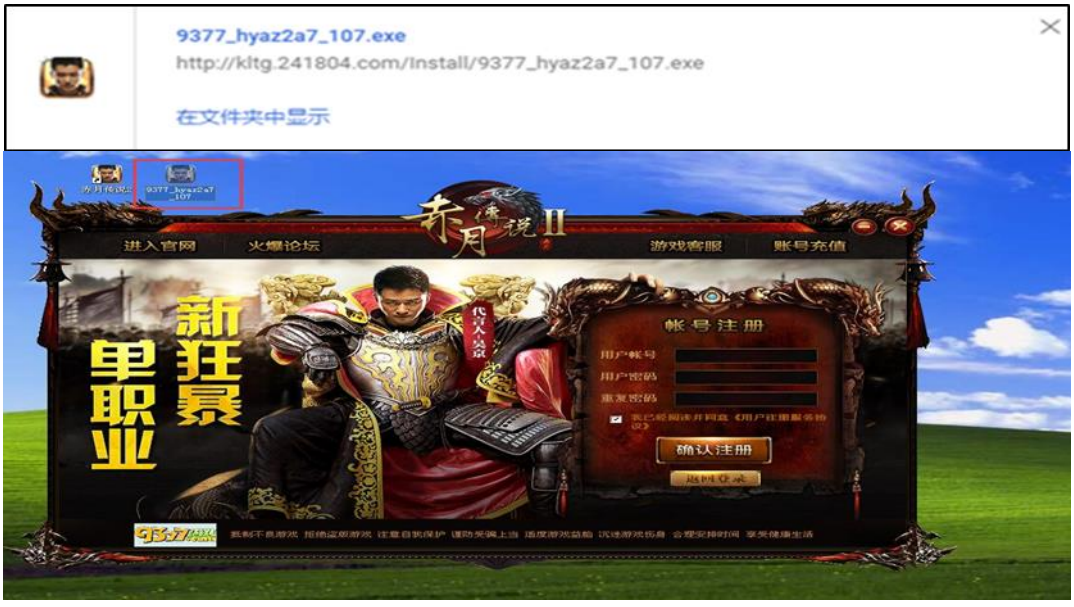


图 4.20 网页挂马事件截图

4.5 网站类安全事件处置建议

【网站类安全事件处置流程】针对网站类安全事件，建议首先清除网站被篡改的内容，找出并删除黑客上传的后门程序，然后对网站进行全面漏洞扫描，找出网站和服务器存在的安全漏洞，对网站源代码和服务器进行漏洞修补和安全加固，必要时重装服务器、重新架设网站。如果存在重要网络和信息系统遭受特别严重的系统损失，重要敏感信息和关键数据丢失或被窃取、篡改或其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁的情况，应立即将有关情况向网络安全主管部门汇报。

【开展网站风险评估工作】网站及重要信息系统在上线前，需做好风险评估工作，网络安全工程师需系统进行全面扫描，排除风险点。没有配备网络安全工程师的单位，可以委托专业的网络安全公司进行风险评估工作。网站及重要信息系统上线运营后，还需定期开展风险评估工作，检测是否存在新型漏洞，发现问题及时解决。

【做好网站安全防护】及时更新网站系统版本；定期扫描网站安全漏洞；定期备份网站数据；购买网站安全防护产品或将网站纳入江苏省网站安全云防护平台。

5、安全漏洞监测情况

5.1 重要信息系统漏洞威胁情况分析

江苏省通信管理局和江苏省互联网应急中心均高度重视对全省各级政府单位和金融、教育等行业重要信息系统的安全威胁预警通报工作。由于绝大部分严重的网络安全威胁都是由信息系统所存在的安全漏洞诱发的，所以及时发现和处理漏洞是安全防范工作的重中之重。

据江苏省互联网应急中心监测统计，2017 年，全省各级党政机关、金融、教育类网站及其他重要信息系统高危漏洞 1131 个，漏洞类型主要包括 SQL 注入、弱口令、远程代码执行等。

据江苏省互联网应急中心统计，全省1131起重要信息系统网站安全漏洞事件中，省级单位发生安全漏洞事件共195起，设区市级610起，区县及以下326起。除省级单位外，苏州、南京、徐州等市安全漏洞事件数居全省前列。江苏省重要信息系统安全漏洞类型分布如图5.1所示，漏洞所属单位行政级别分布如图5.2所示，所属区域分布如图5.3所示。

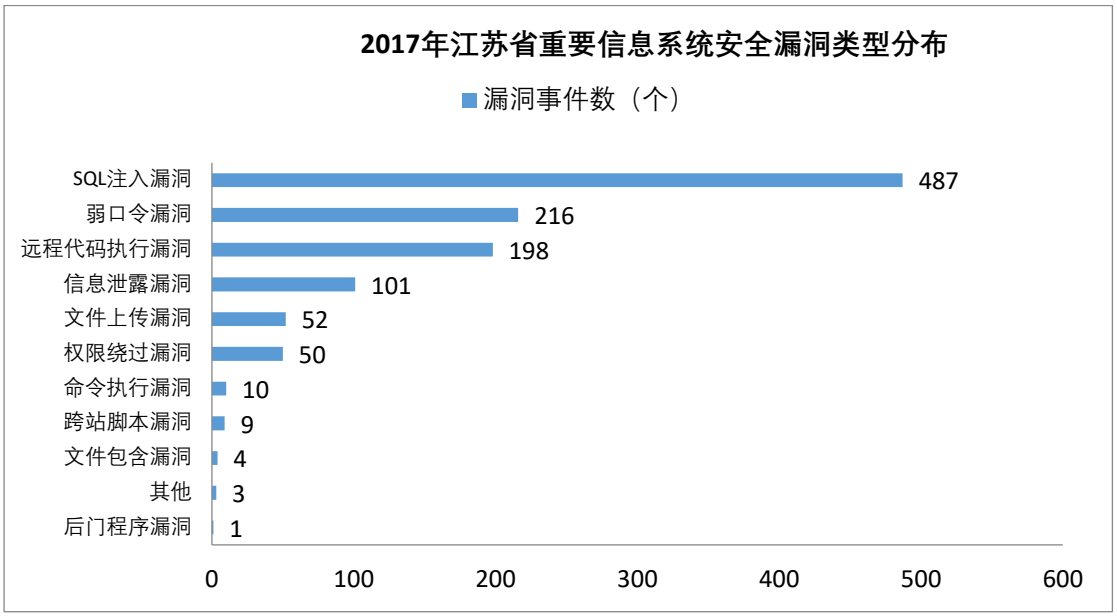


图5.1 2017年江苏省重要信息系统安全漏洞类型分布图

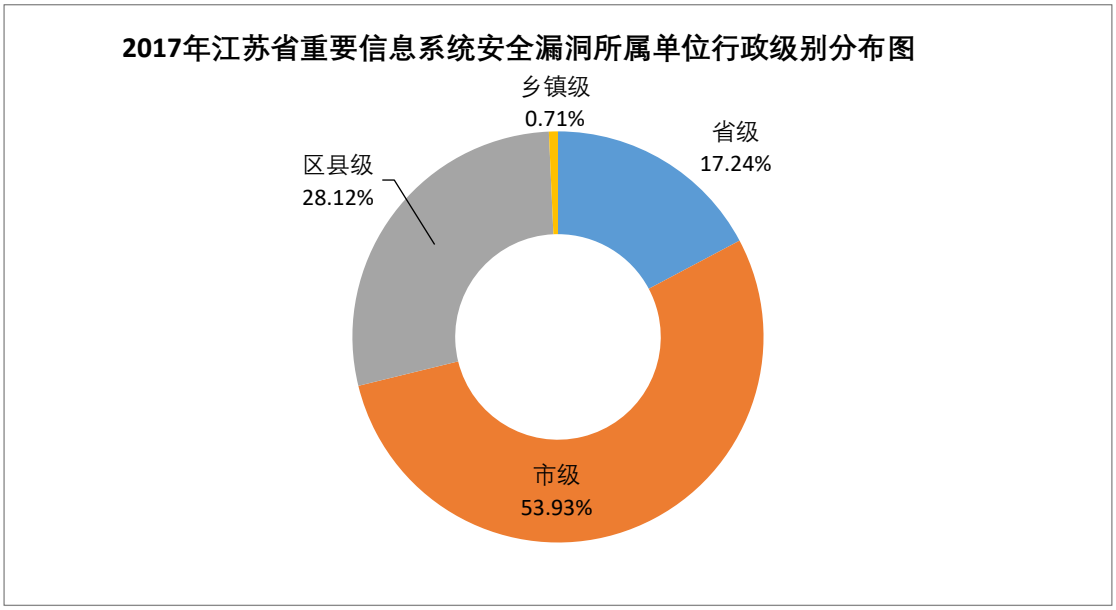


图 5.2 2017 年江苏省重要信息系统安全漏洞所属单位行政级别分布图

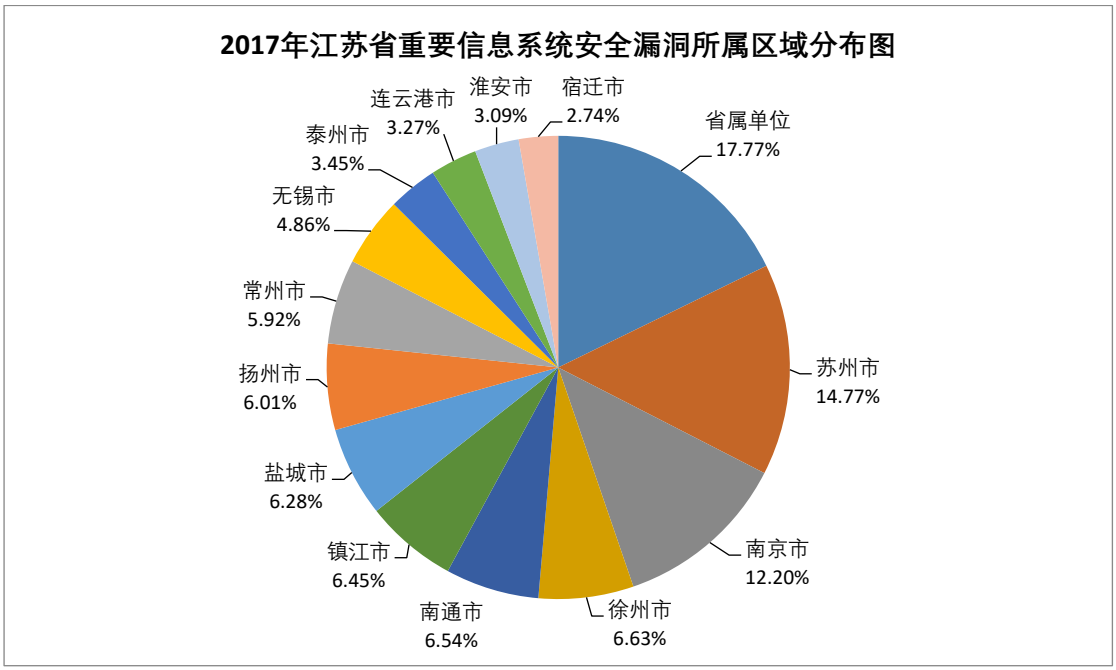


图 5.3 2017 年江苏省重要信息系统安全漏洞所属区域分布图

5.2 WannaCry 勒索病毒席卷全球

5.2.1 事件爆发

2017年5月12日，一款名为WannaCry的蠕虫勒索病毒席卷全球网络，这被认为是迄今为止最大的勒索攻击活动，150余个国家受到网络攻击，受入侵电脑超过20万。该勒索病毒利用了窃取自美国国家安全局（NSA）的黑客工具永恒之蓝（Eternalblue），基于微软445端口的MS17-010漏洞进行自动传播。一旦电

脑感染了WannaCry病毒，受害者电脑内重要文件将会被加密，需支付高达300美元比特币的赎金才可解锁，勒索、文件加密页面分别如图5.4、5.5所示。相关数据显示，病毒爆发初期的一天时间内，国内网络中每小时攻击次数高达4000余次。

图5.4 WannaCry勒索病毒界面

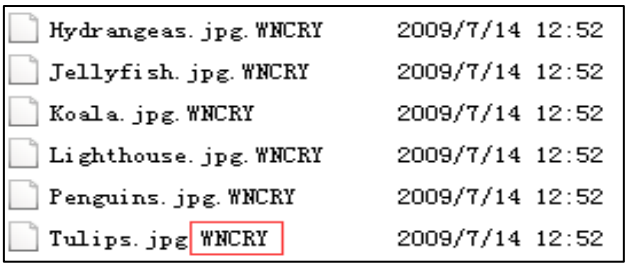


图5.5 文件加密截图

据分析，攻击具备操作系统兼容性、多语言支持，国内多个行业受到影响，国内的ATM机、火车站、自助终端、邮政、医院、政府办事终端、视频监控都可能遭受攻击。报道称，国内部分中石油加油终端和多地公安系统遭到入侵。

图5.6 宿迁部分网站受到勒索病毒影响

5.2.2 事件回顾

WannaCry勒索病毒爆发突然，短短一天内，百余个国家和地区遭受攻击并呈现蔓延态势。但回溯该事件，可以发现攻击并非毫无征兆：

2016年8月，一个名为“影子经纪人（Shadow Brokers）”的黑客组织号称入侵了“方程式（Equation Group）”组织并窃取了大量机密文件，并将部分文件公开到了互联网上，“方程式”据称是美国国家安全局下属的黑客组织，有着极高的技术手段。这部分被公开的文件包括不少隐蔽的地下黑客工具。此外，“影子经纪人”还保留了部分文件，打算以公开拍卖的形式出售，“影子经纪人”预期的价格是100万个比特币，当时价值接近5亿美元。

2017年3月14日，微软发布了一个SMB服务的高危漏洞补丁MS17-010，公告表明“如果攻击者向Windows SMB服务器发送特殊设计的消息，那么其中最严重的漏洞可能允许远程执行代码”。

2017年4月8日，由于前期公开拍卖并未成功，“影子经纪人”公布了保留部分文件的解压缩密码，有人解压缩后将黑客工具上传到Github网站提供下载。

2017年4月14日，继上一次公开解压密码后，“影子经纪人”在其推特（Twitter）上放出了第二波保留的部分文件，此次包括23个新的黑客工具，其中的“永恒之蓝”正是针对MS17-010漏洞设计的攻击方式。江苏省互联网应急中心也于第一时间在网站发布了“关于加强防范Windows操作系统和相关软件漏洞攻击风险的情况公告”（图5.7）。

图 5.7 CNCERT/JS 发布风险预警公告

2017年5月12日，WannaCry勒索病毒全面爆发，并陆续出现变种。由上述时间线，可以看出勒索病毒爆发前两个月，MS17-010高危漏洞的补丁已经发布，病毒爆发前一个月已有公开预警信息，因此信息系统及时升级补丁仍是最有效的防御手段。幸运的是，国内基本屏蔽了公网的445端口，公网受病毒影响相对较小，但内网却成为病毒传播的重灾区，可见内网的安全防护亟待加强。

5.3 全省传播感染情况分析

5.3.1 病毒攻击流程

WannaCry病毒利用“方程式”组织工具包中的“永恒之蓝”漏洞工具，进行网络端口扫描攻击，通过MS17-010漏洞感染其他主机，目标机器被成功攻陷后会从攻击端下载WannaCry病毒进行感染，并作为攻击端再次扫描互联网和局域网其他机器，形成蠕虫感染，大范围快速扩散。

病毒母体为mssecsvc.exe，运行后会扫描随机ip的互联网机器，尝试感染，也会扫描局域网相同网段的机器进行感染传播。此外，会释放敲诈者程序tasksche.exe，对磁盘文件进行加密实施勒索。

病毒使用AES算法加密文件，并使用非对称加密算法RSA 2048加密随机密钥，每个文件使用一个随机密钥，理论上不可破解。整个攻击过程如图5.8所示：

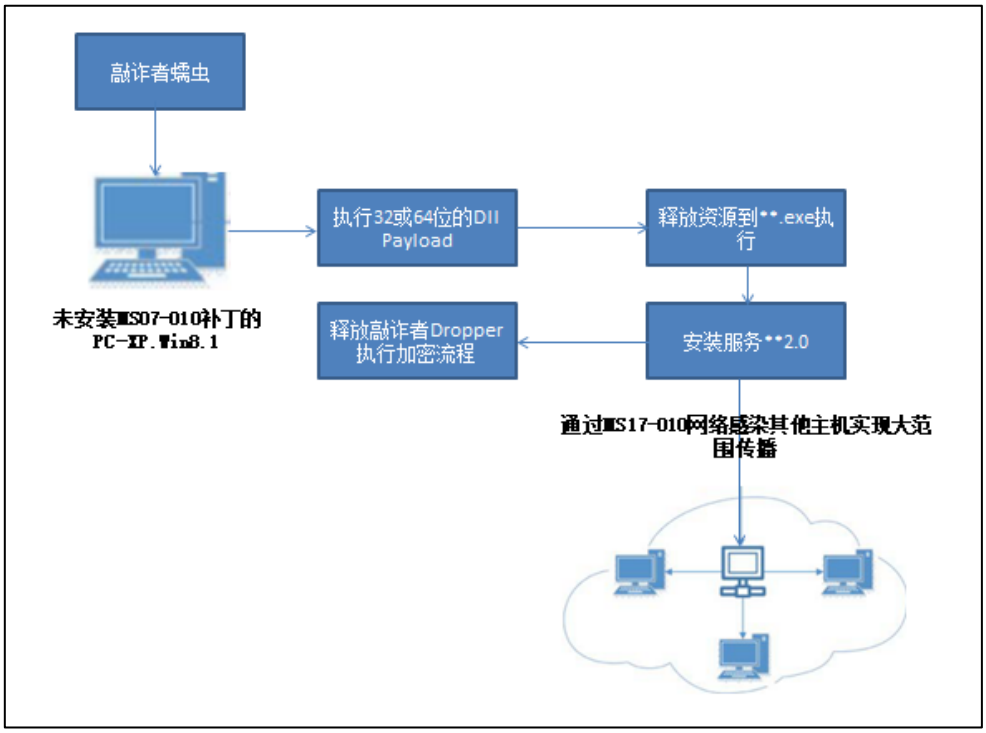


图 5.8 病毒攻击流程

5.3.2 勒索加密过程

病毒会释放一个加密模块到内存，动态获取文件系统和加密相关的 API 函数，以此来躲避静态查杀，整个加密过程采用 RSA+AES 的方式完成，其中 RSA 加密过程使用了微软的 CryptAPI，AES 代码静态编译到 dll。加密流程如下图所示：

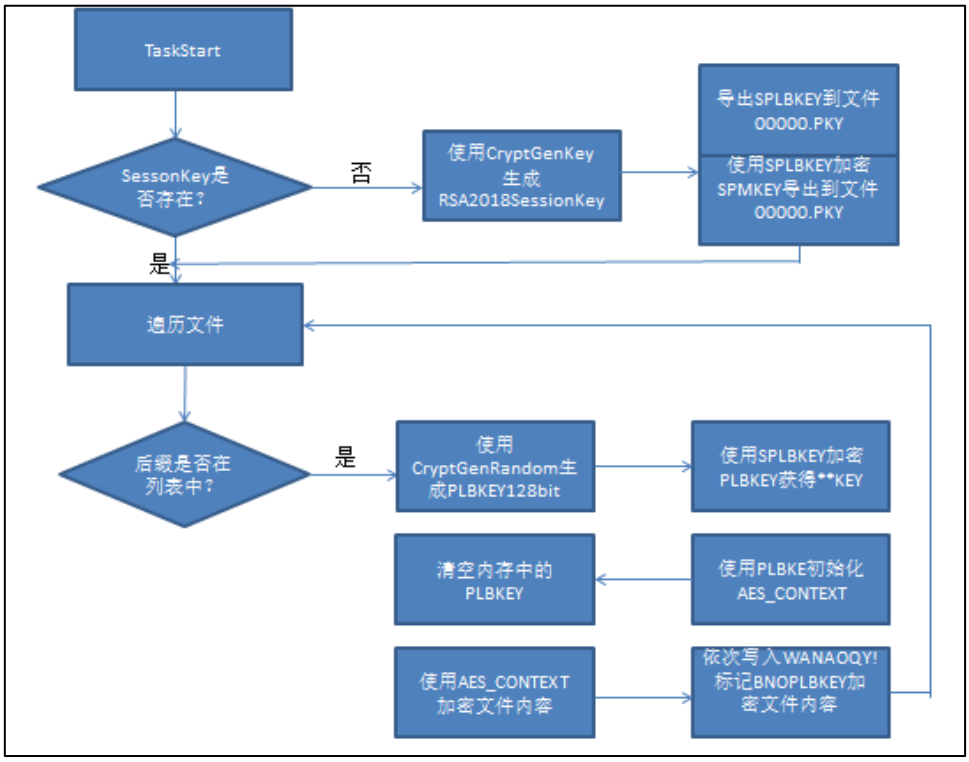
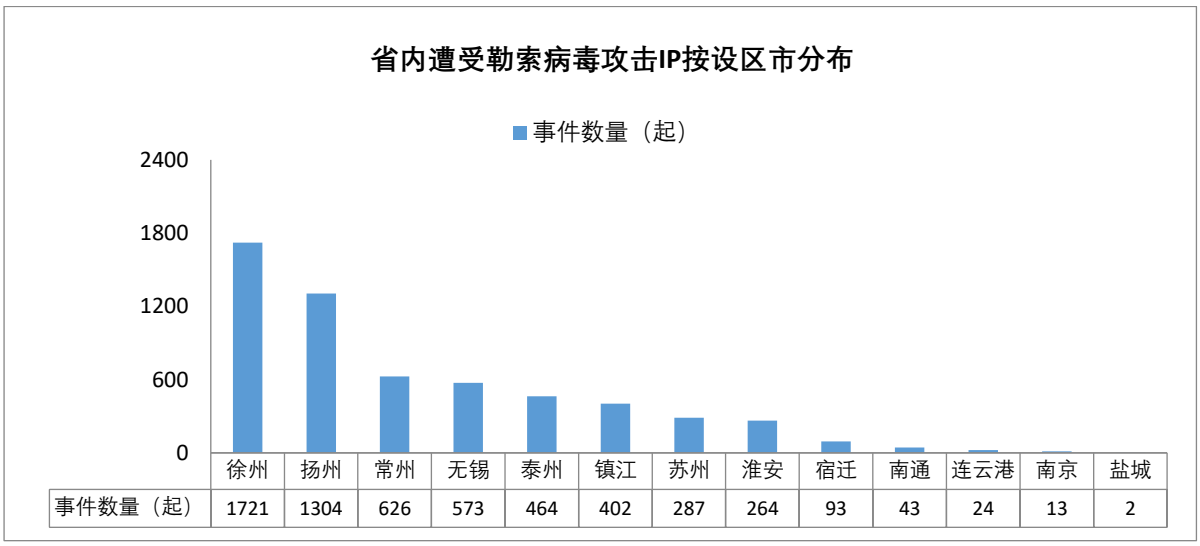


图 5.9 关键勒索加密过程

5.3.3 全省传播感染情况

经江苏省互联网应急中心对全省互联网监测发现，漏洞爆发 48 小时内，省内遭受勒索病毒攻击的 IP 共计 5816 个。其中，徐州、扬州遭受病毒攻击的 IP 数较多，分别为 1721 个、1304 个，其余设区市也均遭到病毒攻击。按设区市统计如图 5.10 所示。



	徐州	扬州	常州	无锡	泰州	镇江	苏州	淮安	宿迁	南通	连云港	南京	盐城
事件数量（起）	1721	1304	626	573	464	402	287	264	93	43	24	13	2

图 5.10 省内遭受勒索病毒攻击 IP 按设区市统计

漏洞爆发 48 小时内，省内发起勒索病毒攻击的 IP 共计 206 个。其中，镇江发起攻击的 IP 数较多，达 158 个，南京、苏州等其他 5 个设区市也存在发起攻击的 IP。按设区市统计如图 5.11 所示。

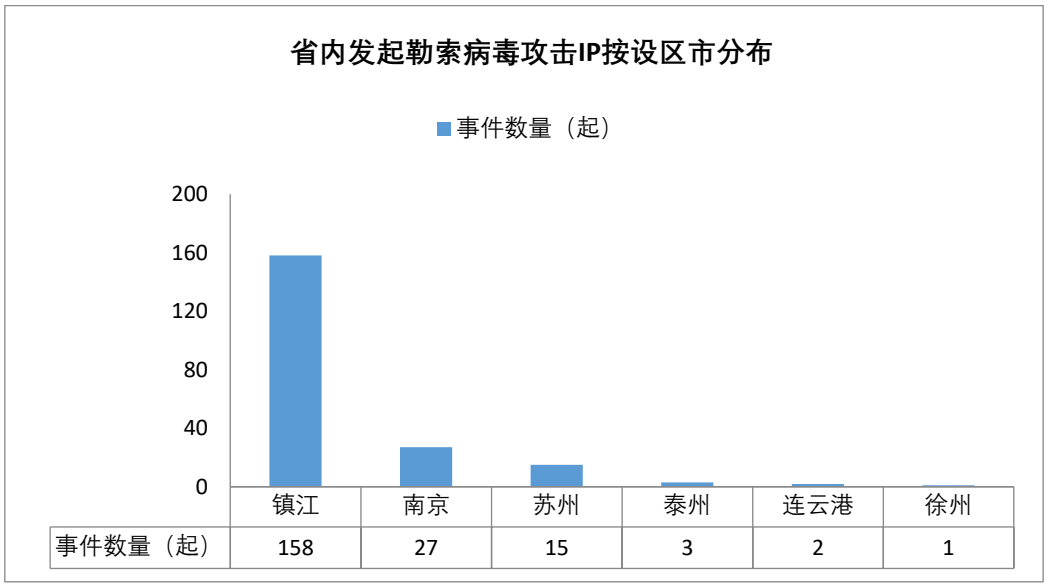


图 5.11 省内发起勒索病毒攻击 IP 按设区市统计

漏洞爆发 48 小时内，省内感染的 IP 共计 393 个。其中，南京、常州、苏州感染的 IP 数较多，分别为 89、82、80 个，其余多个设区市也均存在感染的情况。按设区市统计如图 5.12 所示；

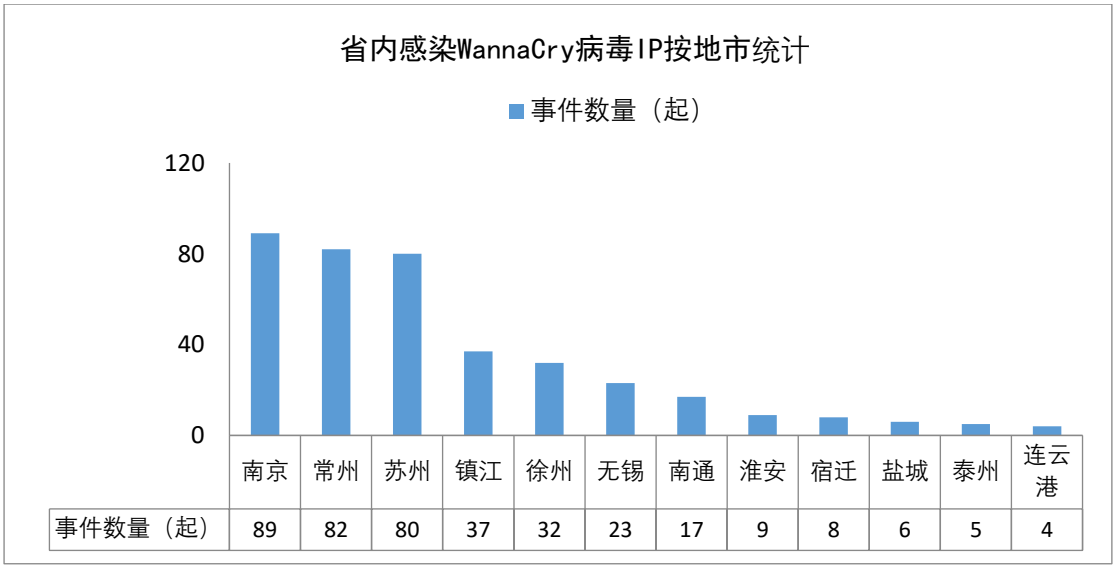


图 5.12 省内感染 WannaCry 病毒 IP 按设区市统计

6、网络安全专题分析

6.1 网络安全威胁治理专题

2017年，江苏省用户主机感染僵尸木马病毒、网络流量攻击、网站渗透攻击、数据窃取、网页篡改等各类网络安全事件仍频繁发生，为保障互联网用户的个人信息安全、财产安全，维护全省互联网和重要信息系统平稳，江苏省通信管理局、江苏省互联网应急中心全年持续开展针对高频次僵尸木马控制端、受控端、蠕虫病毒、网站后门的专项打击清理工作。同时，随着大数据、云计算、物联网、人工智能相关业态的发展及应用，网络安全威胁治理工作已经到了一个新的阶段，如何应用人工智能、大数据分析等技术手段，挖掘网络安全攻击事件、提升监测和处置能力是网络安全工作人员面临的新课题。

6.1.1 净化互联网环境，加强网络安全威胁治理工作

常态化工作方面，针对僵尸网络攻击、DDoS攻击高发态势，2017年江苏省互联网应急中心持续开展僵尸木马蠕虫病毒、网站挂马事件等专项处置任务22次，共协调处置网络安全事件32.79万起。全年共发现党政机关网站和重要信息系统高危漏洞1131个，发送网络安全事件处置函186份。突发事件应急处置工作方面，5月12日，“永恒之蓝”勒索病毒爆发，我省共有5816个IP地址遭受攻击，6月上旬，木马病毒“暗云III”在互联网大规模传播，我省共有10.03万个IP地址感染病毒。上述事件发生后，江苏省互联网应急中心第一时间组织研判，加强监测，协调运营企业和责任主体处置事件，并对外发布风险预警，做好应急响应，保障省内关键信息基础设施安全稳定运行。

6.1.2 “扫黄打非”，清理省内违法违规网站

2017 年，根据工业和信息化部与省“扫黄打非”工作领导小组的相关要求和统一部署，江苏省通信管理局集合信息通信全行业力量开展“扫黄打非·净网2017”等互联网专项整治行动，按照“突出重点、落实责任、技管结合、务求实效”的原则，全力以赴做好网上淫秽色情、涉恐涉暴等违法信息治理。以互联网为主战场，坚持专项治理与综合治理相结合，严厉打击淫秽色情文化垃圾、违

法违规网络直播平台、非法弹窗、微领域网络平台、网站、云盘等传播淫秽色情文学作品和信息以及利用新闻客户端传播庸俗、低俗、媚俗内容行为。全年江苏省通信管理局累计完成 20.66 万个备案信息审核工作，注销和清理空壳网站 4.63 万个，配合关闭淫秽色情网站 184 个；组织全省基础电信企业排查梳理网站 2 万余家，清理不良信息数据 1.23 万条，互联网“扫黄打非”工作进一步得到深化。

6.2 工业互联网安全专题

6.2.1 背景介绍

工业互联网是指全球工业系统与高级计算、分析、感应技术以及互联网连接融合的结果。它通过智能机器间的连接并最终将人机连接，结合软件和大数据分析，重构全球工业，激发生产力。随着我国大力推进信息化建设，工业控制系统在我国各行业的应用范围和部署规模快速增长，工业控制系统已成为国家关键信息基础设施的“中枢神经”。我国近几年工业控制系统的网络安全事件屡有发生，如钢厂异常停机、炼油厂系统异常等等，这些层出不穷的安全事件，为我国关键信息基础设施核心系统的安全问题敲响了警钟。

6.2.2 案例分析

下面以某市工业监控系统为例。该系统负责市内多个大中型工业系统的监控。然而，系统存在管理员弱口令、敏感数据泄露等安全风险，这些监控视频一旦被犯罪分子掌握和利用，后果不堪设想。该市矿井、化工企业等区域监视频截图如图 6.1、6.2、6.3 所示。

图 6.1 某矿井内部监控可发现用于爆破的危险物品（图像已处理）

图 6.2 某企业监控截图（图像已处理）

图 6.3 某单位办公区域监控截图（图像已处理）

造成该市多个区域监控视频外泄风险的主要原因有两点：一是监控系统的管理服务器直接暴露在了互联网上，可被远程访问；二是监控系统服务器的管理员帐号使用了弱口令，弱口令为该视频监控系统服务商设置的初始密码。

6.2.3 应对措施

工控安全事关经济发展、社会稳定和国家安全，应对新时期工控安全形势，提升工业互联网安全防护水平，江苏省互联网应急中心建议：

（1）在工业主机上采用在离线环境中充分验证测试的防毒软件或者应用程序白名单软件，只允许经过工业自身授权和安全评估的软件运行；

（2）建立防病毒和恶意软件入侵管理机制，对工业控制系统及临时接入的设备采取病毒查杀等安全预防措施；

（3）做好工业控制网络、工业主机和工业控制设备的安全配置，建立工业控制系统配置清单，定期进行配置审计；

（4）对重大配置变更制定变更计划并进行影响分析，配置变更实施前进行严格安全测试；

（5）密切关注重大工控安全漏洞及其补丁发布，及时采取补丁升级措施。在补丁安装前，需对补丁进行严格的安全评估和验证测试。

6.3 DDoS 攻击事件专题

6.3.1 背景介绍

2017 年 7 月，据支撑单位安天公司上报，发现一种具备拒绝服务（DDoS）攻击能力的新型木马。经初步分析，该木马属于一个新家族，并将其命名为“魔鼬”。通过关联查询 DDoS 攻击的历史监测数据，发现本次事件中受攻击的域名同时也在遭受 Trojan/Linux.BillGates、Trojan/Linux.Mayday 等家族的 DDoS 攻击。

6.3.2 案例分析

通过样本分析，发现被攻击域名或 IP 多为操作系统下载站点，受攻击的域名/IP 和对应的网站名如图 6.4 所示。

域名/IP	网站名
win7.bdxsa.com	系统之家
www.swerrt.cn	系统之家
x1.xy1758.com	
www.xiaomaxitong.cn	小马一键重装系统
win7.hangzhouhongcaib.cn	无法访问
win.geelai.cn	系统下载
xz.xamy119.com	小猪一键重装系统
xm.0537yiyao.com	小马一键重装系统
blog.xy1758.com	
win7.yahung5.com	系统之家
win7.shangshai-qibao.cn	系统下载
183.134.16.11	
43.230.72.134	
14.152.83.24	

图 6.4 受攻击的域名/IP 对应的网站

通过在部分网络出口提取攻击数据，部分域名访问量抽样统计如图 6.5、6.6 所示：

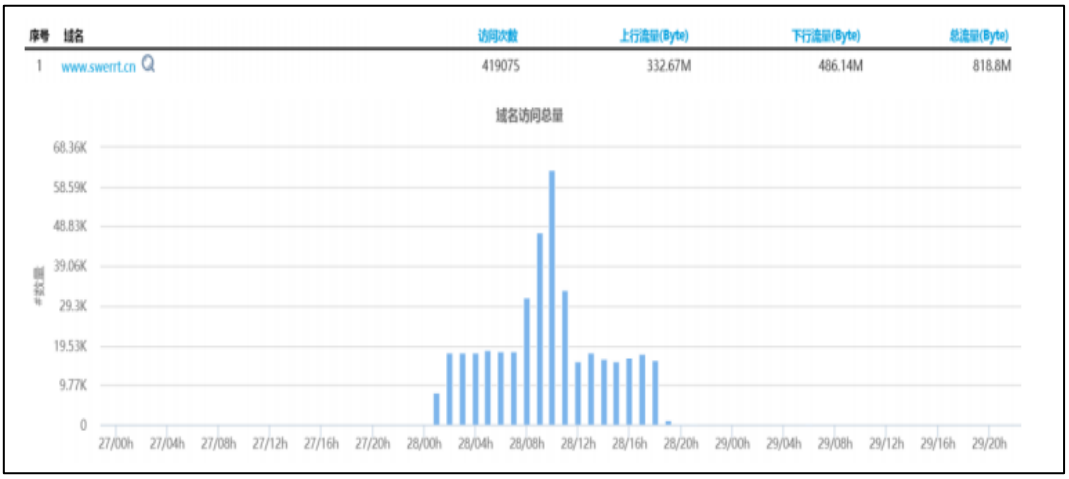


图 6.5 对 www.swerrt.cn 域名的访问量截图

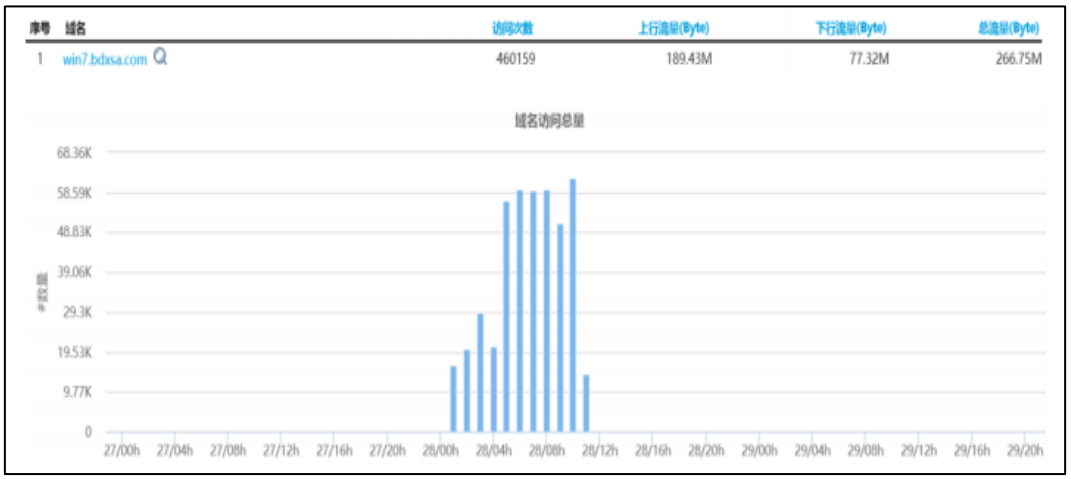


图 6.6 对 win7.bdxsa.com 域名的访问量截图

【事件样本分析】

样本的编译时间为 2017-07-01 21:22:54，根据前面的攻击事件发现时间，初步认为该时间是未经过篡改的，可见该木马家族出现时间仅有短短的 1 个月。

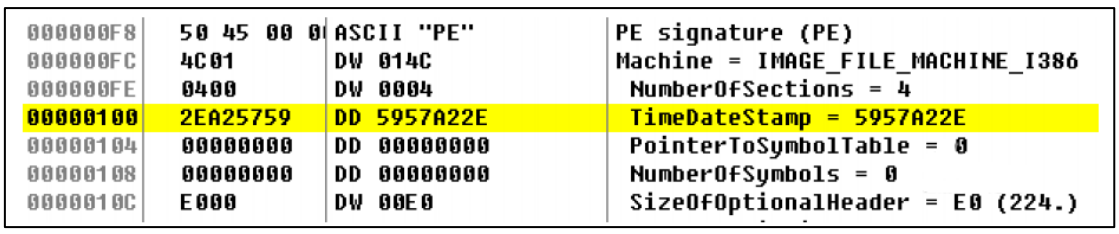


图 6.7 样本时间戳截图

样本的运行流程和主要行为如下：

（1）创建互斥量保证唯一实例运行截图如下：

```
call    sub_401130
push    offset a73b66e4c194a4a ; "{73B66E4C-194A-4af1-B541-BF3DC3FB3ED5}"
push    0               ; bInitialOwner
push    0               ; lpMutexAttributes
call    ds:CreateMutexA
mov     esi, eax
call    ds:GetLastError
test    esi, esi
jz      short loc_4011F4
cmp     eax, 0B7h
jnz     short loc_4011F4
mov     ecx, [esp+58h+var_4]
pop     edi
pop     esi
pop     ebx
xor     ecx, esp
xor     eax, eax
call    @__security_check_cookie@4 ; __security_check_cookie(x)
mov     esp, ebp
```

图 6.8 创建互斥量截图

（2）加载资源数据，读取指定偏移的内容作为 C&C 地址（www.linux288.com）。

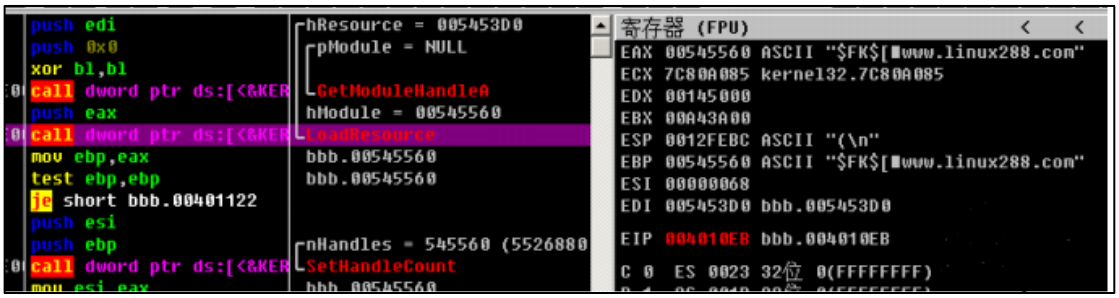


图 6.9 加载资源数据截图

（3）连接 C&C 服务器，发送本机系统信息（包括主机名、CPU、内存、系统版本等），接收 C&C 返回的攻击目标列表截图如下：

```
                        ; CODE XREF: sub_40D4B0+293Tj
mov     eax, [esi+18h]
lea     edx, [esp+948h+readfds]
push    edx             ; fd_set *
push    eax             ; fd
call    __WSAFDIsSet
test    eax, eax
jz      short loc_40D899
mov     edx, [esi+18h]
push    0               ; flags
push    800h            ; len
lea     ecx, [esp+950h+buf]
push    ecx             ; buf
push    edx             ; s
call    ds:recv         ; 接收远程服务器返回的数据（待攻击地址列表）
cmp     eax, 1
jl      short loc_40D8C5
mov     edx, [esi]
mov     edx, [edx+8]
push    eax
lea     eax, [esp+94Ch+buf]
push    eax
mov     ecx, esi
call    edx
```

图 6.10 接受服务器返回数据截图

（4）在分析中我们发现，C&C 返回的攻击目标列表数据每隔一段时间会发生变化，从而控制受害主机向不同的 IP 或域名发动攻击。服务器返回不同的攻击目标列表截图如下：

图 6.11 服务器返回不同的攻击目标列表

（5）接收到数据后，样本按指定的格式解析攻击列表数据（link_list 和 task_list）截图如下：

```
push    offset aTask_list ; "task_list"
lea     esi, [eax+4]
mov     [ecx+4], bl
call    sub_4015E0
mov     ecx, esi
call    sub_415310
add     esp, 1Ch
cmp     al, bl
jz      loc_40C665
push    9
push    offset aTask_list ; "task_list"
lea     ecx, [esp+98h+var_4C]
mov     [esp+98h+var_34], edi
mov     [esp+98h+var_38], ebx
mov     byte ptr [esp+98h+var_48], bl
call    sub_4015E0
lea     ecx, [esp+90h+var_4C]
push    ecx
mov     ecx, esi
mov     byte ptr [esp+94h+var_4], 1
call    sub_40DAC0
mov     edx, [eax]
push    ebx
push    offset off_53FD80 ; int
push    offset off_53FD6C ; int
push    ebx             ; int
push    edx             ; int
call    sub_41A92A
```

图 6.12 解析数据包内容截图

（6）样本根据 task_list 地址和配置，创建大量线程，向目标地址发起 DDoS 攻击，截图如下：

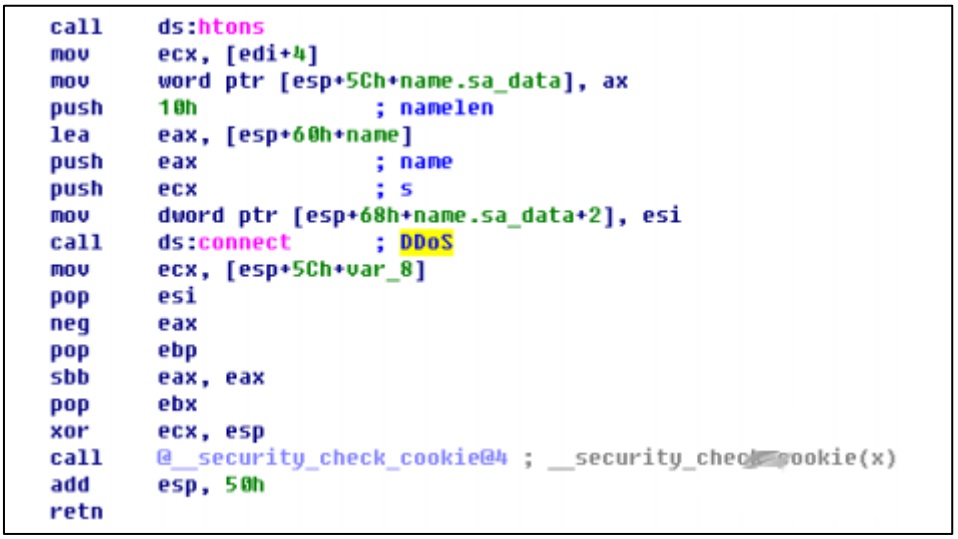


图 6.13 发起 DDoS 攻击截图

经过分析和关联查询，发现在相近时间内多个组织对相同目标发起 DDoS 攻击。从目前掌握的资料来 看，本次 DDoS 事件的攻击强度足以打瘫一般的网站，但是部分受攻击网站采用了 CDN 服务，因此网站访问没有受到严重影响。该木马家族出现的 1 个月内，发现多起由该家族发起的 DDoS 攻击事件，说明木马传播速度较快，需要引起重视。

6.3.3 应对措施

物联网、云计算等技术的普及已深刻影响着 DDoS 攻防形势，我们面临的安全防护形势更加严峻。DDoS 攻击从最初基于 PC 机的僵尸网络攻击，到近两年盛行的反射放大攻击，再到现在越来越多的基于云主机、物联网设备的僵尸网络攻击，我们看到 DDoS 攻击规模不断扩大，攻击算法更加智能。各种攻击服务的产业化，也使得发起复杂、大规模攻击的门槛大大降低，近年多起破坏力巨大的 DDoS 攻击事件已经给互联网安全敲响了警钟。江苏省互联网应急中心建议：

（1）保证充足的网络带宽，网络带宽直接决定了设备抗受攻击的能力；

（2）在网络带宽保证的前提下，尽量提升系统的硬件配置；

（3）采用高性能的网络设备，使得网络设备不成为系统性能瓶颈；

（4）条件允许的情况下，将系统接入专业 DDoS 攻击防护平台。

6.4 物联网设备安全专题

6.4.1 背景介绍

蓝牙协议作为物联网设备常用的通信协议之一，随着物联网时代的开启，使用蓝牙协议的设备数量日益增多。近期，物联网安全公司 Armis Labs 披露了一个攻击向量 BlueBorne，称攻击者可利用一系列与蓝牙相关的安全漏洞，在一定场景下可实现对具有蓝牙功能的远端设备的控制，进而窃取受害者数据、进行中间人攻击以及在感染一个设备后蠕虫式感染其它设备，且此攻击方式无需向用户申请认证授权，具有较大的危害性。

蓝牙协议是中短距离无线通信采用的常用协议，但由于其规则庞大、架构复杂、功能模块繁多，且一些功能允许厂商自定义，直接导致很多蓝牙设备并未选择相对安全的加密通信方式；另外，一些设备由于自身性质原因，无法执行特定身份认证过程（例如蓝牙耳机无法执行“密钥输入”安全模式，因为耳机设备上就没有可供键盘输入的接口）。这是造成此次蓝牙安全威胁的两大直接原因。

6.4.2 案例分析

蓝牙协议栈的主要模块及此次安全威胁的漏洞分布情况：

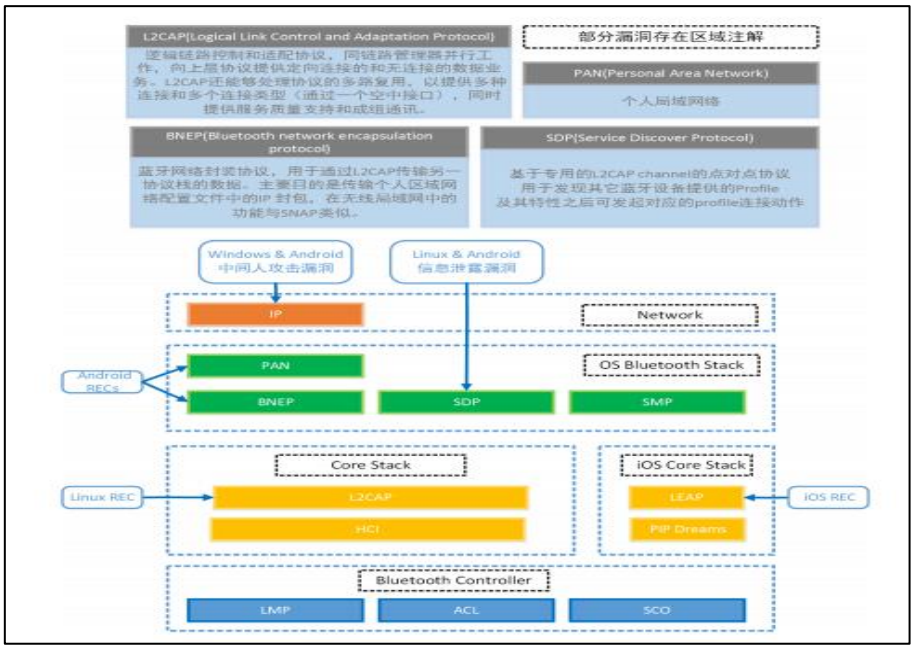


图 6.14 蓝牙协议漏洞分布情况

Linux 内核的远程控制执行漏洞(CVE-2017-1000251)，攻击者可利用此溢出漏洞向蓝牙协议发送畸形数据包，对目标设备进行恶意配置，为下一步攻击做准备。

蓝牙协议栈信息泄露漏洞(CVE-2017-1000250)，由于蓝牙协议在设计规范方面存在不足，导致基于 SDP 模块的“续传模式”在上述内核溢出漏洞存在的前提下，在部分 Linux 与 Android 系统中会被攻击者完全控制，进而执行进一步的堆溢出攻击。

Android 信息泄露漏洞(CVE-2017-0785)，类似于在蓝牙协议栈上的漏洞，利用 SDP 服务器的一个记录数目整数值的下溢出漏洞，攻击者可进而利用“续传模式”在 Android 设备上反复传输指令，达到绕过计数验证 ASLR(Address space layout randomization，内存空间地址随机化）保护机制的效果。

蓝牙协议引入了的 SSP（Secure simple pairing，简化安全配对）安全模式，提供了如下四种认证方式：

安全认证方式	应用场景
“数据比较”认证 (Numeric Comparison)	两个蓝牙设备都有显示6位数字的能力并允许用户输入“是”或“否”响应
“只比较不确认认证” (Just Works)	至少有一个配对设备既没有显示也没有键盘来输入数字（例如:耳机）
“密码输入认证” (Passkry Entry)	一个蓝牙设备具有输入能力（例如:键盘）而另一个设备有显示但没有输入能力
“外带认证”OOB认证 (Out of Band)	支持共同的额外无线或有线技术（例如:近场通信或NFC）来作为设备发现和加密值交换

图 6.15 SSP 认证方式

因为很多蓝牙设备自身或待连接的远端设备不具有外置输入接口以及显示能力，故会采用“只比较不确认认证”的方式，而此方式无法进行可靠的身份认证过程。攻击者在攻击采用 Android 系统的设备（一些 Android 系统版本有效）时，其利用场景就是基于对方设备具备显示和输入能力，但攻击者设备不具备输入和显示能力（攻击者可自行构造此状态）的情况下，可以远程发起一个无需与目标设备的用户进行交互的连接请求，接着建立连接并通信；对于采用 Windows 操作系统的设备（一些 Windows 系统版本有效），攻击者采用同样的原理，发起构造的“无输入和显示能力-无需 MITM（Man in the Middle，中间人攻击）防护”的连接请求，接着完成认证并进行后续通信。因为攻击者已经完成身份认证，而蓝牙在几乎所有操作系统中都具有最高权限，因而攻击者具有访问很多高权限服务的能力，进而实现对目标设备的进一步控制。

6.4.4 应对措施

物联网设备的安全问题需要采取一个全新专业化安全方案来解决：互联网上的所有设备必须为其用户提供相应级别的安全保障。物联网中复杂的混合技术组件（数据中心、云、网络、软件、硬件）都必须高度安全，江苏省互联网应急中心建议：

（1）用户自行将系统升级至最新版本，并及时安装更新补丁。对安全要求高的用户，若对应系统/补丁暂未发布，建议请等待系统更新或补丁升级后再使用蓝牙设备；

（2）因蓝牙属于中短距离无线通信协议，不建议在安装更新和补丁前在公共场合等非信任场景下使用蓝牙设备；

（3）建议不使用蓝牙共享网络（包括 BNEP 和 PAN）；

（4）面对无外接输入和显示功能的设备（如部分蓝牙耳机、蓝牙鼠标等），在无法信任此设备或无法确定此设备是否安全时（如路边某咖啡厅的蓝牙音响），不要主动连接。

6.5 APT 攻击事件专题

6.5.1 背景介绍

APT攻击（Advanced Persistent Threat，高级持续性威胁）是利用先进的攻击手段对特定目标进行长期持续性网络攻击的形式。APT攻击的原理相对于其他攻击形式更为高级和先进，其高级性主要体现在精确的信息收集、高度的隐蔽性、以及使用各种复杂的目标系统、应用程序漏洞等方面。在传统的认知中，APT活动应该是比较隐蔽的，通常不易被察觉。但在2017年，APT组织及其活动与网络空间中的大国博弈呈现出很多微妙的显性联系。

2017年，被APT攻击次数最多的国家依次是：美国、中国、沙特阿拉伯、韩国、以色列、土耳其、日本、法国、俄罗斯、德国、西班牙、巴基斯坦和英国这13国家。

表6.1 被APT攻击次数最多的国家及领域列表

被攻击目标国家	攻击组织数量	主要被攻击领域
美国	7	政府、能源、IT/互联网、媒体、航天、金融、酒店
中国	7	政府、互联网、军队、电信、媒体、航天、金融、科研

沙特阿拉伯	4	政府、能源、IT/互联网、军队、航天、化工、大型企业
韩国	5	互联网、金融、能源、交通
以色列	5	政府、IT/互联网、媒体、航天、军队、电信、金融、大型企业
土耳其	2	政府、能源、工业、大型企业、军队
日本	3	政府
法国	2	政府
俄罗斯	2	政府、金融
德国	3	政府、军队、大型企业、IT

通过对相关研究报告分析发现，在2017年，APT组织最为关注的机构类型是政府，50%的APT组织以政府为攻击目标；其次是能源行业，受到25%的APT组织关注。排在APT组织攻击目标前十位的重要领域还有金融、国防、互联网、航空航天、媒体、电信、医疗、化工等。

2017年，针对我国境内目标发动攻击的境内外APT组织达38个，目前仍高度活跃的至少有6个。统计显示，2017年全年，这些APT组织发动的攻击行动，至少影响了我国境内上万台主机，攻击范围遍布国内31个省级行政区。下表给出了部分针对我国境内目标发动攻击的APT组织活动情况。

表6.2 针对中国境内目标攻击的部分APT组织活动情况

组织	主要攻击手法	已知最早活动时间	最近活动时间
海莲花（APT-C-00）	鱼叉攻击、水坑攻击	2012年	2018年2月
Darkhotel（APT-C-00）	鱼叉攻击	2014年	2017年9月
摩诃草（APT-C-09）	鱼叉攻击	2009年	2018年2月
APT-C-12	鱼叉攻击	2014年	2017年10月
APT-C-56	鱼叉攻击	2014年	2018年2月
APT-C-58	鱼叉攻击渗透	2011年	2017年12月

2017年，国内受APT攻击最多的地区是辽宁、北京、山东、江苏、上海、浙江和广东等。关于APT攻击在中国境内的分布情况，详见下图（不含港澳台地区）。

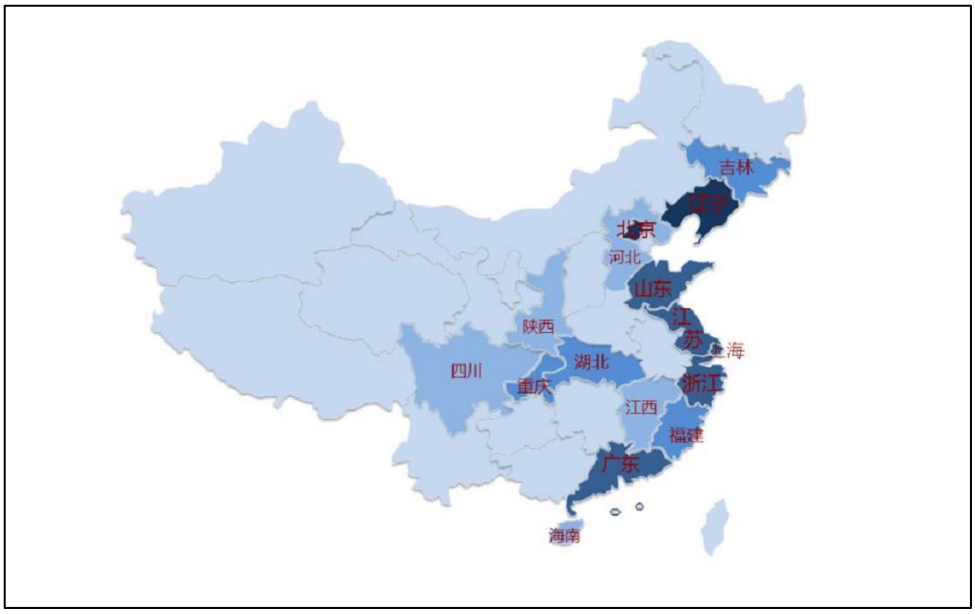


图6.16 APT攻击在中国境内的分布情况

6.5.2 典型 APT 组织分析——海莲花

基于对样本及各上报厂家的数据源整合分析和历史活动的长期跟踪，发现海莲花组织活动的一些变化。

（1）木马对抗性更强更复杂

海莲花先后使用过多种形态的专用木马，虽然均是以窃取感染目标主机中的机密数据为目的，2017 年，部分较新的恶意代码利用了系统中白名单程序 MSBuild.exe 来执行恶意代码以绕过查杀。这种加载恶意代码的方式本质上与利用带正常签名的 PE 程序加载位于数据文件中的恶意代码方法相同。

（2）木马攻击面收窄，更具针对性

与 2016 年相比，海莲花组织的攻击活动面有所收窄，但攻击目标的针对性加强，对攻击目标了解更加深入。有用户提供的样本使用了如下的附件名：invitation letter-zhejiang ***** working group.doc，星号是非常具体的目标所在组织的简称，目标人物在浙江省，所以附件名里加了 zhejiang 字样，暗示这是完全对目标定制的攻击木马，这体现了攻击者对攻击目标的专注度。

（3）服务器更加隐蔽更难追踪

为了隐藏自己的真实身份，海莲花组织经常变换下载服务器和 C&C 服务器的域名和 IP。而且大多数域名为了抵抗溯源都开启了 Whois 域名隐藏，使得分析人员很难知道恶意域名背后的注册者是谁。在 2017 年 11 月最新的样本中还

使用了 DGA 算法以进一步逃避检测，这就大大增加了安全分析人员定位有效服务器难度。

（4）持续瞄准高价值客户

海莲花组织似乎不甘心丢掉之前已经攻陷的“目标”而选择“卷土重来”。例如，对之前已经攻击过的目标会进行反复攻击，发送新版本的鱼叉攻击[3]，并尝试再次获取控制。此外，在某些仍然被控制着的电脑终端上，海莲花组织的攻击者也会通过推送新的木马程序，将木马的 C&C 服务器转换到新的 IP 或域名下。

6.5.3 APT 活动与网络空间大国博弈

在传统的认知中，APT 活动应该是比较隐蔽的，通常不易被察觉。但在 2017 年，APT 组织及其活动，则与网络空间中的大国博弈之间呈现出很多微妙的显性联系。这种联系主要表现在以下五个方面。

（1） APT 行动与国家间的政治摩擦密切相关

2017 年，某些具有极强的国别针对性的 APT 组织，在相关国家处于比较激烈的政治和军事摩擦时，其网络攻击活动也处于异常活跃的状态。其中，双尾蝎、黄金鼠和摩诃草等组织在 2017 年的攻击活动都呈现出这样的特点。

（2） APT 行动对于地缘政治的影响日益显著

2016 年底进行的美国大选，以及希拉里和美国民主党全国委员会（DNC）的邮件门事件，使公众第一次见证了 APT 攻击对地缘政治，乃至国家政权的深刻影响。美国作为世界第一强国，互联网第一强国，却成为世界上第一个明确因受 APT 攻击而直接影响大选结果的“受害国”。

2017 年 5 月，ESET、FireEye 等安全机构发布报告称发现 APT28 干扰法国总统大选，对法国大选候选人马克龙等发动“鱼叉攻击”，其中还同时使用到了 Office 和 Windows 的 0day 漏洞。仅就攻击技术的复杂度和先进性而言，针对法国大选的攻击活动要比美国大选的邮件门事件高出了几个层次。

（3） 指责他国的 APT 活动已成重要外交手段

朝鲜政府 2017 年与美国的关系十分紧张，一度双方口水战甚至扬言要兵戎相见，而且半岛南北政府之间关系也十分微妙，加上周边国家地缘政治十分复

[3]鱼叉攻击：是黑客攻击方式之一，最常见的做法是，将木马程序作为电子邮件的附件，并起上一个极具诱惑力的名称，发送给目标电脑，诱使受害者打开附件，从而感染木马。

杂，让这一地区的 APT 活动蒙上了更加隐秘的色彩。2017 年 5 月，WannaCry 病毒刚刚爆发，就有研究机构声称是朝鲜“制造”了这起大规模的网络破坏活动，但遭到了朝鲜政府的断然否认。2017 年 10 月和 12 月，英国政府和美国政府再次明确指称是朝鲜制造了 WannaCry 病毒，似乎是坐实了要把始作俑者扣在朝鲜黑客的头上。2017 年 12 月 22 日，朝鲜外交部针对 WannaCry 事件作出回应称：“美国这一举动属于严重的政治挑衅，目的是妖魔化朝鲜，从而促使国际社会对朝鲜进行对抗。”虽然美国政府宣称已经获得了证据，但目前仍未公开任何实质性证据。

（4） APT 组织针对国家智库的攻击显著增多

在当前国际地缘政治格局中，智库通常在政策制定、策略研究等方面扮演重要角色，也和国家政治高层来往密切，因此也成为众多 APT 组织尝试渗透和攻击的重要目标之一，尤其是关注政治决策、政策动向的 APT 组织。

2017 年以来，针对智库攻击的 APT 活动再次增多。根据影子经纪人公布的美国方程式组织的资料文档中，中国.cn 域名遭到的攻击最多，其中包括清华大学、中国科学院等著名智库机构都是方程式组织重点攻击的目标。预计未来，随着国际政治的演变更加复杂化，各个政府对研究机构、政策智库的依赖也将加大，APT 组织针对各个国家的智库的攻击会越来越多。

7、重点行业互联网安全状况分析

2017 年，据江苏省互联网应急中心统计，全省各类网络安全事件中，涉及教育行业 4950.65 万起；涉及党政机关 1835.04 万起；涉及金融行业 107.49 万起。各行业网络安全事件分布如图 7.1 所示。

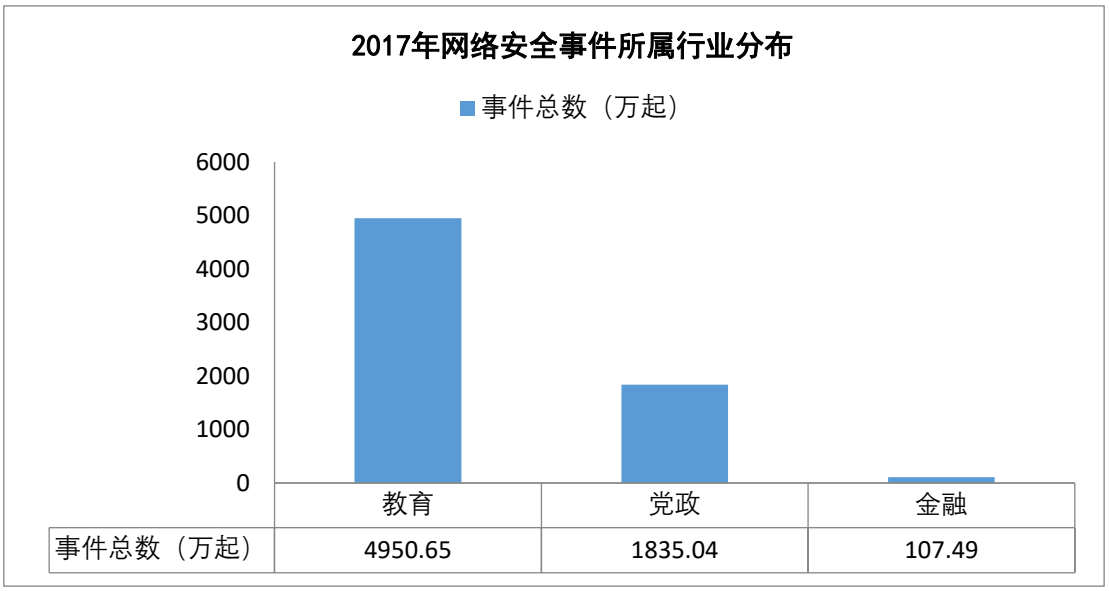


图 7.1 2017 年江苏省网络安全事件所属行业分布图

7.1 党政机关互联网安全状况

2017 年，据江苏省互联网应急中心统计，全省各级党政机关发生各类网络安全事件 1835.04 万起。其中，僵尸木马受控事件 1830.79 万起、飞客蠕虫事件 2.32 万起，僵尸木马控制事件 1.79 万起，网站漏洞事件 1131 起，网页篡改事件 352 起，党政机关网络安全事件类型分布如图 7.2 所示。

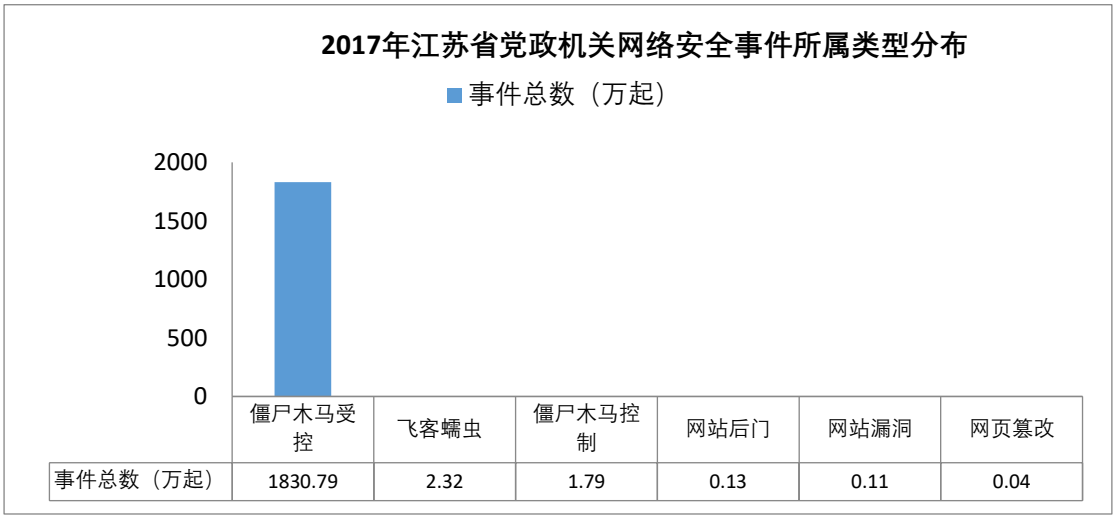


图 7.2 2017 年江苏省党政机关网络安全事件分布图

【主机安全状况】

2017 年，江苏省党政机关发生主机类安全事件共 1834.89 万起，其中僵尸木马受控事件 1830.79 万起，涉及 IP 地址 552 个；蠕虫病毒事件 2.32 万起，涉及 IP 地址 370 个；僵尸木马控制端事件 1.79 万起，涉及 IP 地址 17 个。党政机关主机类安全事件情况如图 7.3 所示。

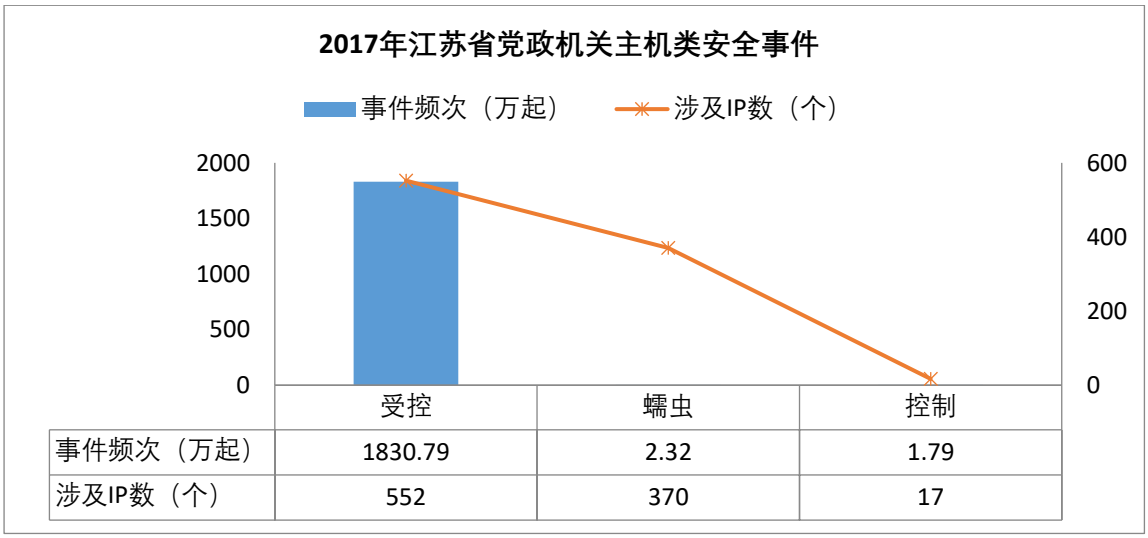
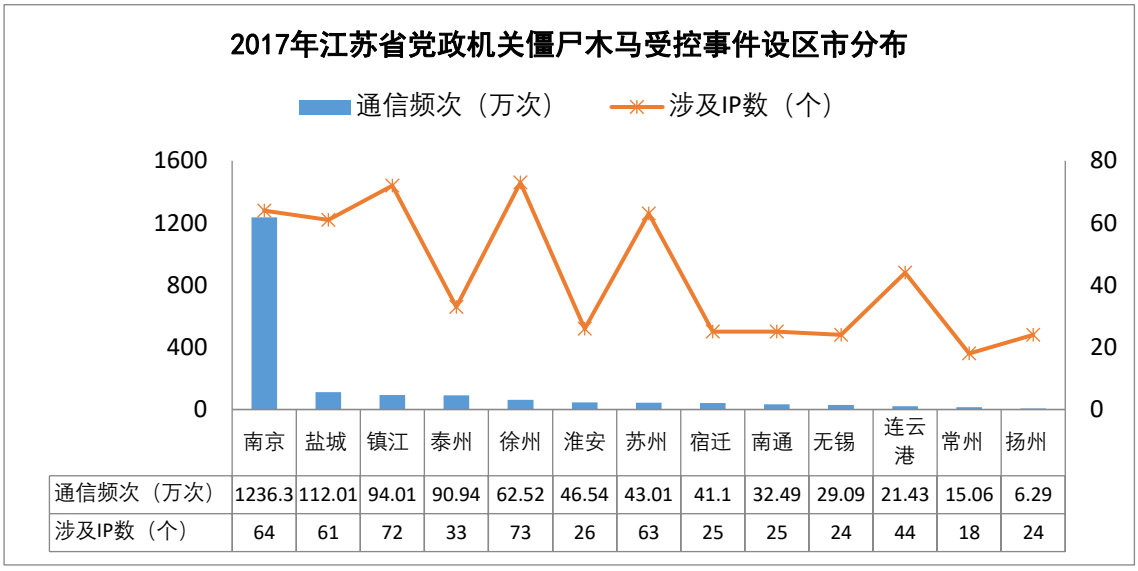


图 7.3 2017 年江苏省党政机关主机类安全事件分布

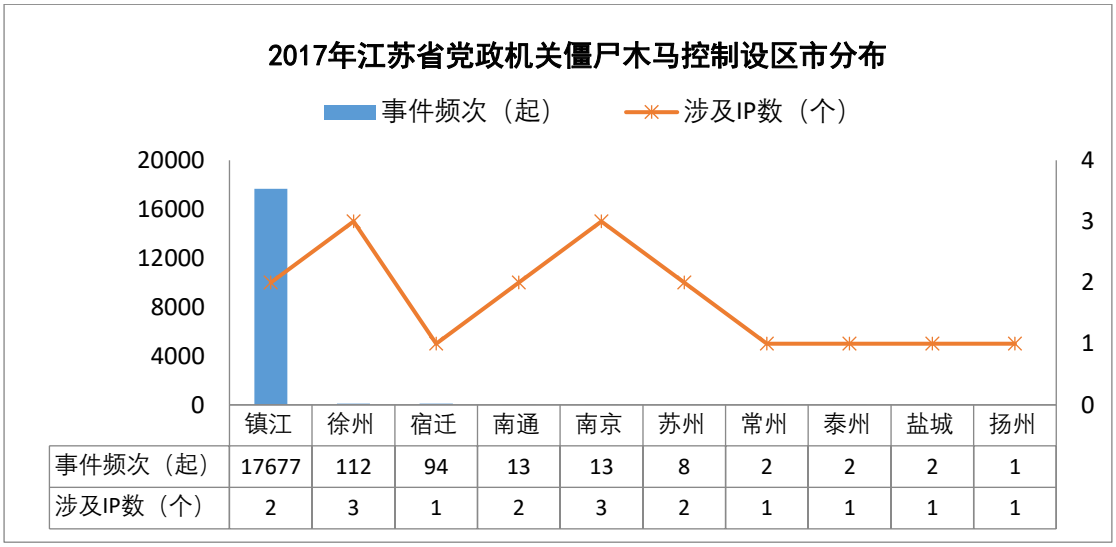
党政机关主机感染僵尸木马事件前三的城市分别为南京、盐城、镇江，感染主机与控制端通信频次分别为 1236.31 万起、112.01 万起、94.01 万起，2017 年江苏省党政机关僵尸木马受控事件设区市分布如图 7.4 所示。



	南京	盐城	镇江	泰州	徐州	淮安	苏州	宿迁	南通	无锡	连云港	常州	扬州
通信频次（万次）	1236.3	112.01	94.01	90.94	62.52	46.54	43.01	41.1	32.49	29.09	21.43	15.06	6.29
涉及IP数（个）	64	61	72	33	73	26	63	25	25	24	44	18	24

图 7.4 2017 年江苏省党政机关僵尸木马受控事件区域分布图

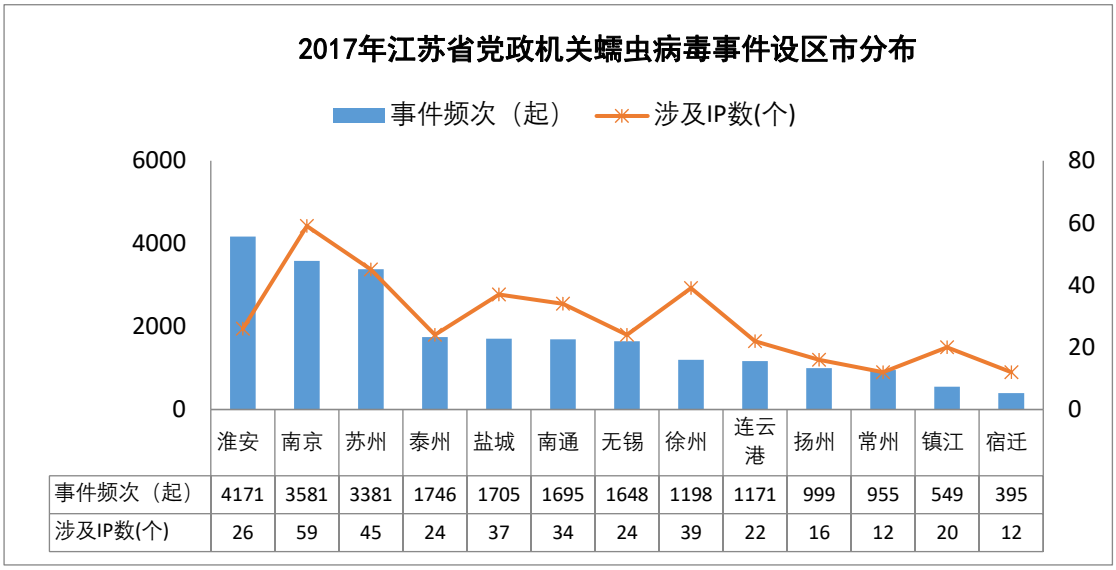
党政机关主机作为僵尸木马控制端与受控主机通信频次数量最多的设区市是镇江，事件频次为 17677 起。2017 年江苏省党政机关僵尸木马控制事件设区市分布如图 7.5 所示。



	镇江	徐州	宿迁	南通	南京	苏州	常州	泰州	盐城	扬州
事件频次（起）	17677	112	94	13	13	8	2	2	2	1
涉及IP数（个）	2	3	1	2	3	2	1	1	1	1

图 7.5 2017 年江苏省党政机关僵尸木马控制事件设区市分布图

党政机关感染蠕虫病毒事件排名前三的城市分别为淮安、南京、苏州，事件频次分别为 4171 起、3581 起、3381 起。2017 年江苏省党政机关蠕虫病毒感染事件分布如图 7.6 所示。

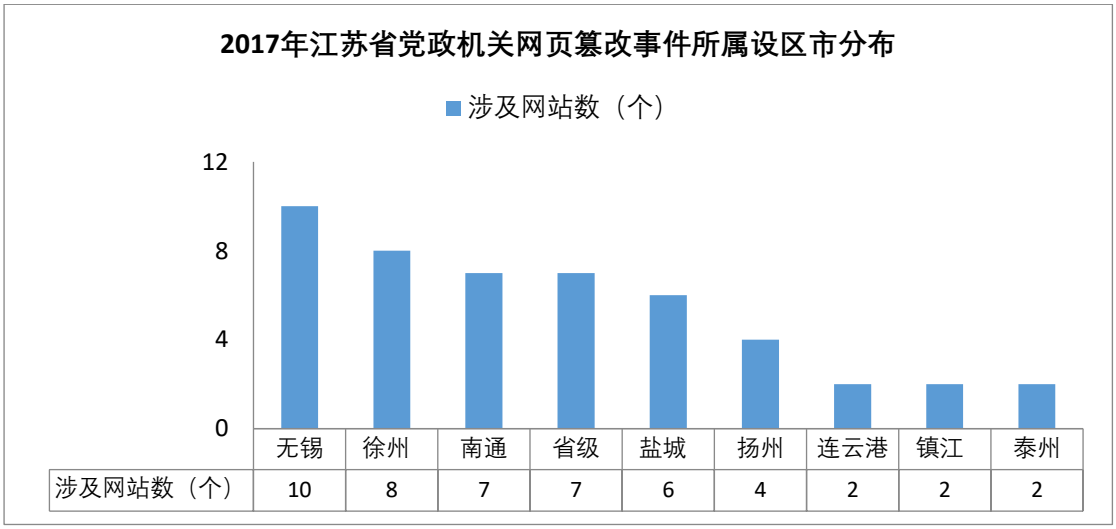


	淮安	南京	苏州	泰州	盐城	南通	无锡	徐州	连云港	扬州	常州	镇江	宿迁
事件频次（起）	4171	3581	3381	1746	1705	1695	1648	1198	1171	999	955	549	395
涉及IP数(个)	26	59	45	24	37	34	24	39	22	16	12	20	12

图 7.6 2017 年江苏省党政机关蠕虫病毒事件设区市分布图

【网站安全状况】

2017 年，江苏省党政机关发生网页篡改事件 352 起，涉及 56 个网站，其中 7 个省级单位的网站遭篡改，设区市级以下被篡改网站 49 个。网页篡改类型集中在广告链接和网站黑页，其中，广告链接型篡改占总事件的 98%。2017 年江苏省党政机关被篡改网站所属设区市分布如图 7.7 所示。



	无锡	徐州	南通	省级	盐城	扬州	连云港	镇江	泰州
涉及网站数（个）	10	8	7	7	6	4	2	2	2

图 7.7 2017 年江苏省党政机关网页篡改事件所属设区市分布图

2017 年，江苏省党政机关发生网站后门事件 1330 起，涉及 43 个网站，南京是发生网站后门事件最多的设区市。黑客利用网站或主机存在的漏洞在服务器上传后门，利用后门控制服务器。2017 年江苏省党政机关被植入后门网站所属设区市分布如图 7.8 所示。

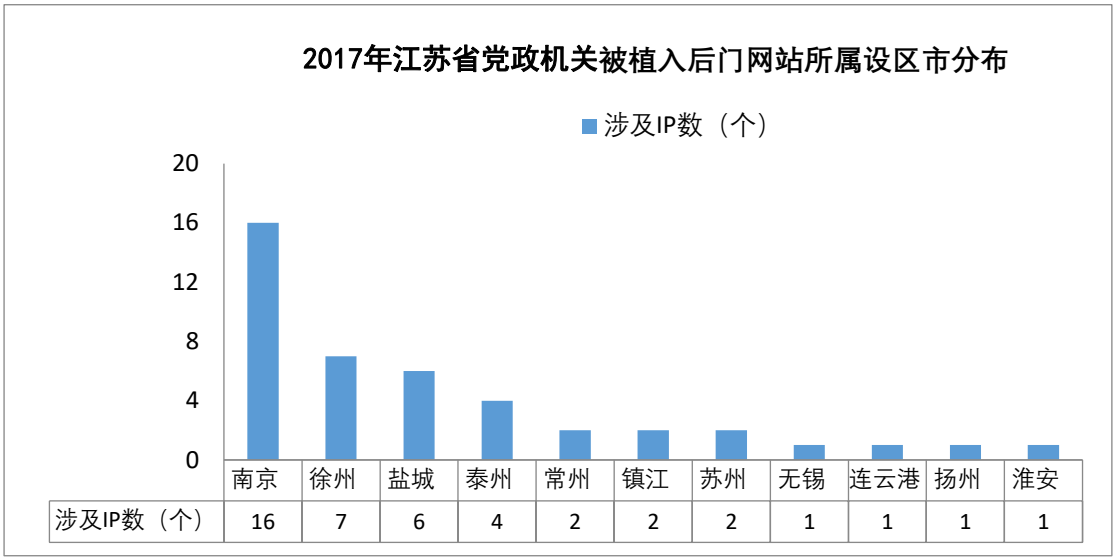


图 7.8 2017 年江苏省党政机关注入后门网站所属设区市分布图

【网站漏洞事件】

2017 年，据国家互联网应急中心（CNCERT/CC）和国家信息安全漏洞共享平台（CNVD）通报，并经江苏省互联网应急中心验证，共发现全省党政机关网站存在各类安全漏洞 1131 个，同比下降 2.92%。其中省级单位网站存在安全漏洞 195 个，设区市单位网站存在安全漏洞 610 个，区县及以下单位网站存在安全漏洞 415 个。除省级单位外，苏州、南京、徐州党政机关网站安全漏洞数居全省前列，分别为 201 个、167 个和 138 个。网站漏洞类型主要集中在 SQL 注入、弱口令、远程代码执行，其中 SQL 注入漏洞事件 487 起，占总漏洞事件的 43.06%。2017 年江苏省各级党政机关网站漏洞事件按单位级别分布、所属设区市分布、漏洞类型分布和月度分布，分别如图 7.9、7.10、7.11 和 7.12 所示。

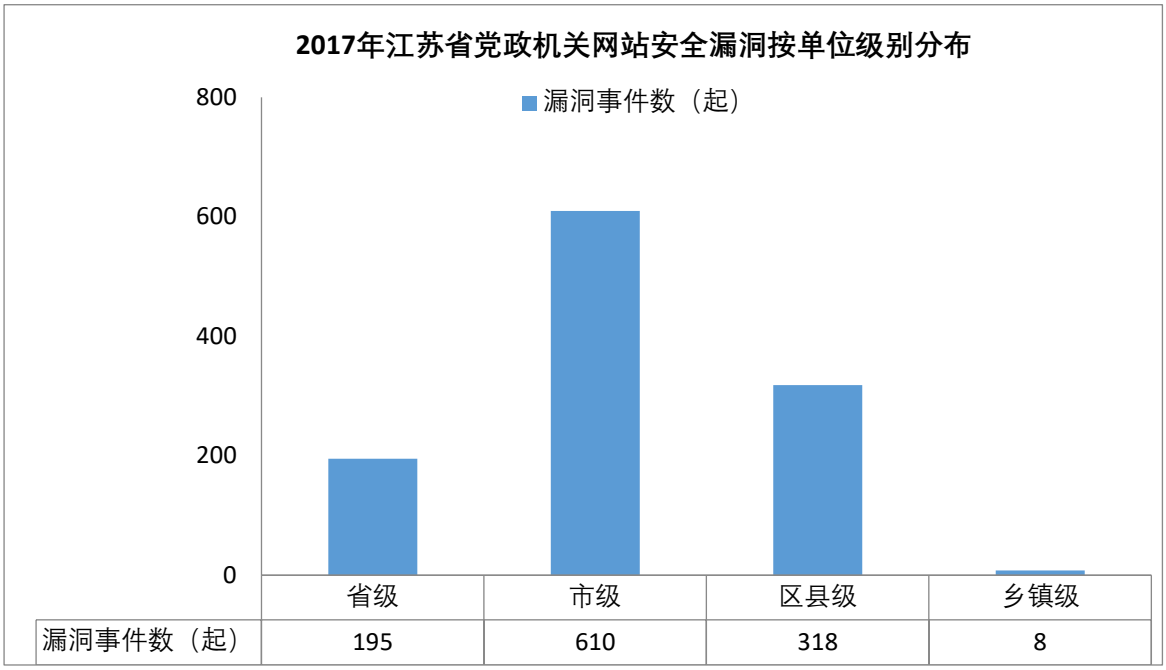


图 7.9 2017 年江苏省党政机关网站安全漏洞按单位级别分布图

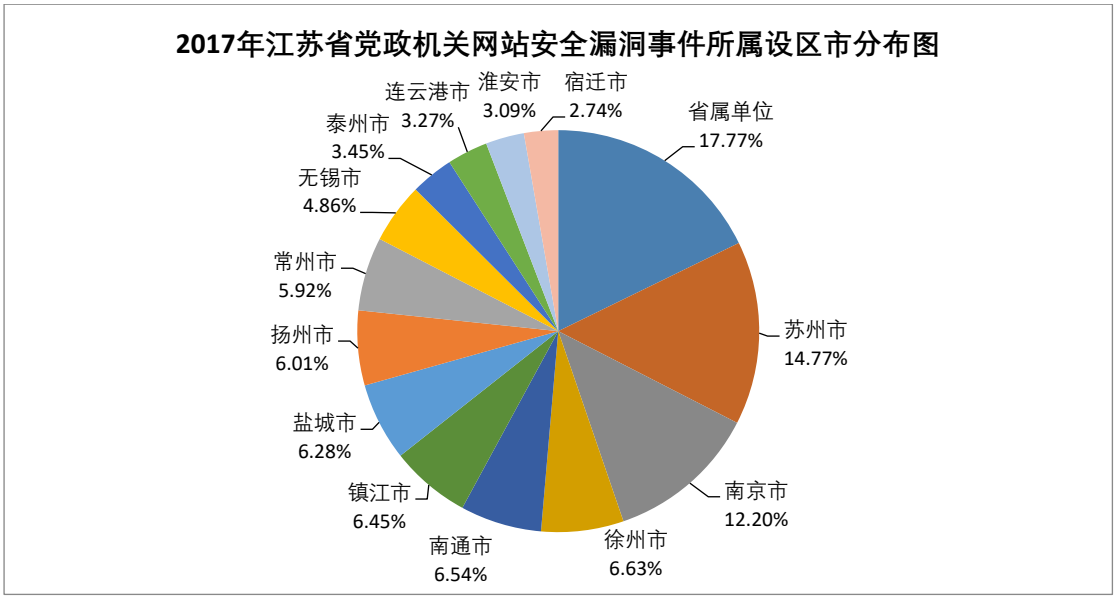


图 7.10 2017 年江苏省党政机关网站安全漏洞事件所属设区市分布图

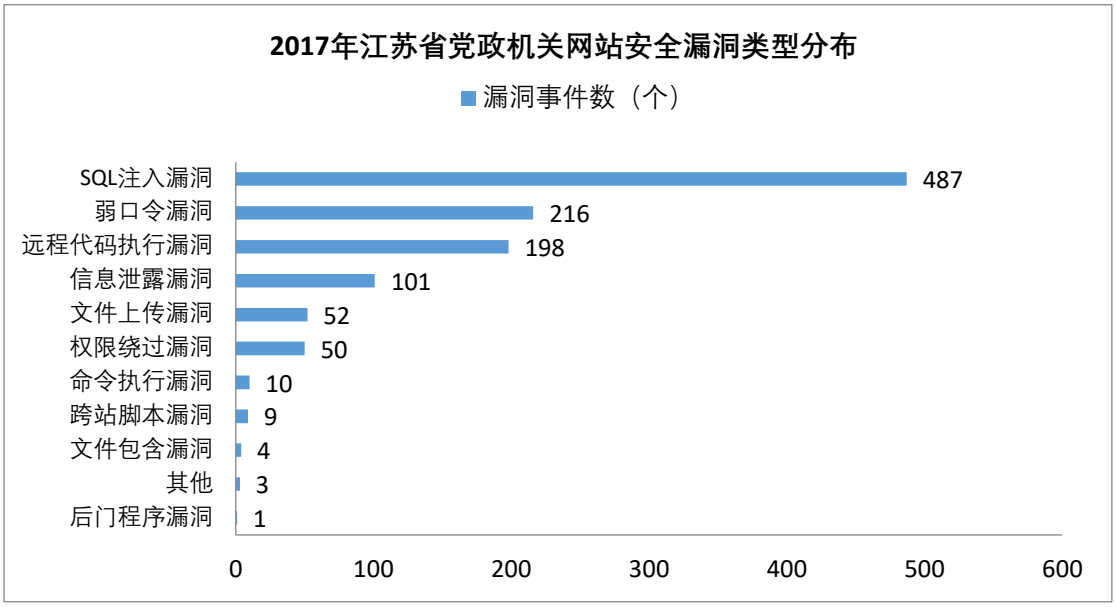
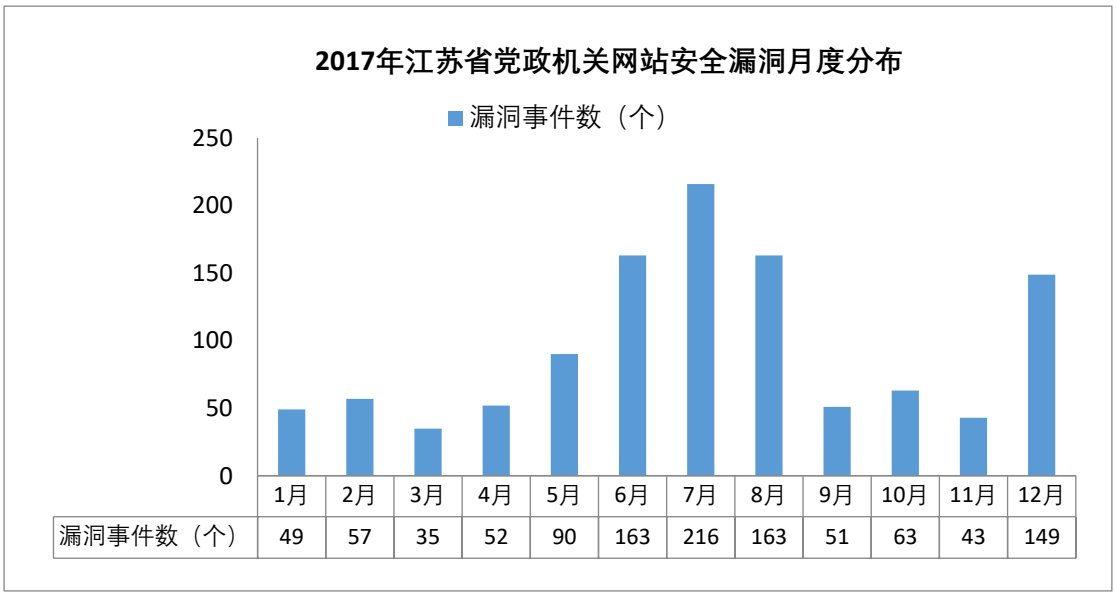


图 7.11 2017 年江苏省党政机关网站安全漏洞类型分布图



	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
漏洞事件数（个）	49	57	35	52	90	163	216	163	51	63	43	149

图 7.12 2017 年江苏省党政机关网站安全漏洞月度分布图

7.2 金融行业互联网安全状况

2017 年，据江苏省互联网应急中心统计，江苏省银行、保险、证券等金融行业共发生主机类网络安全事件 107.49 万起。其中，发生僵尸木马受控事件 106.75 万起，飞客蠕虫事件 7393 起，僵尸木马控制事件 35 起。2017 年金融行业主机类网络安全事件分布如图 7.13 所示。

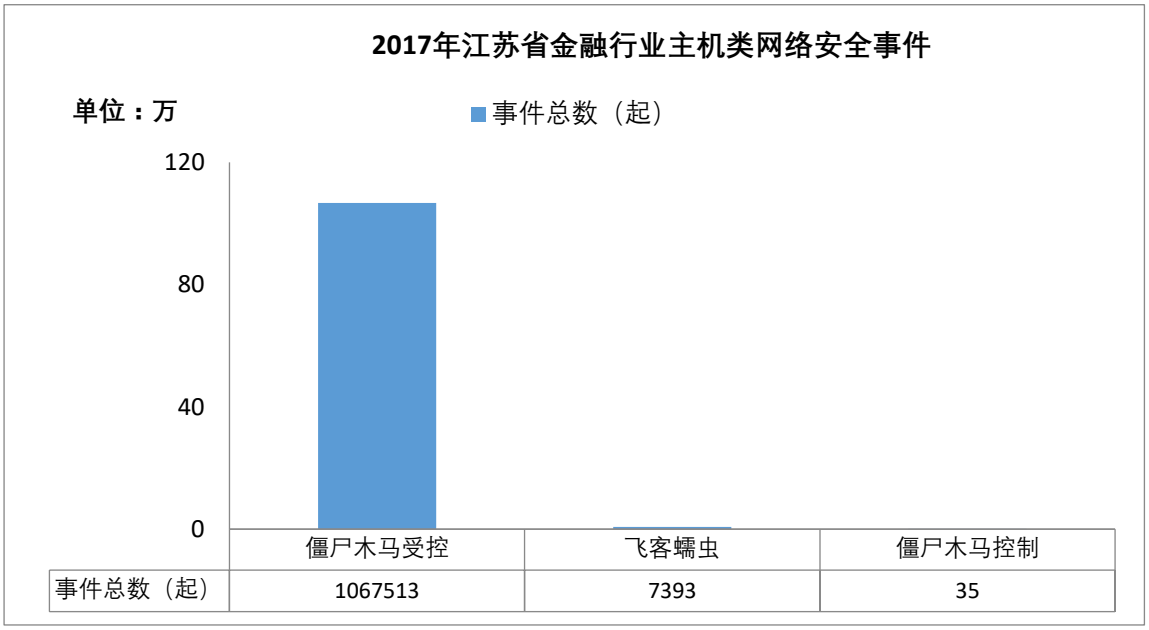


图 7.13 2017 年江苏省金融行业主机类网络安全事件分布图

作为僵尸木马控制端主机的金融部门为投资公司、保险和银行，其中投资公司控制事件数为 30 起。金融部门中僵尸木马控制事件主要分布如图 7.14 所示。

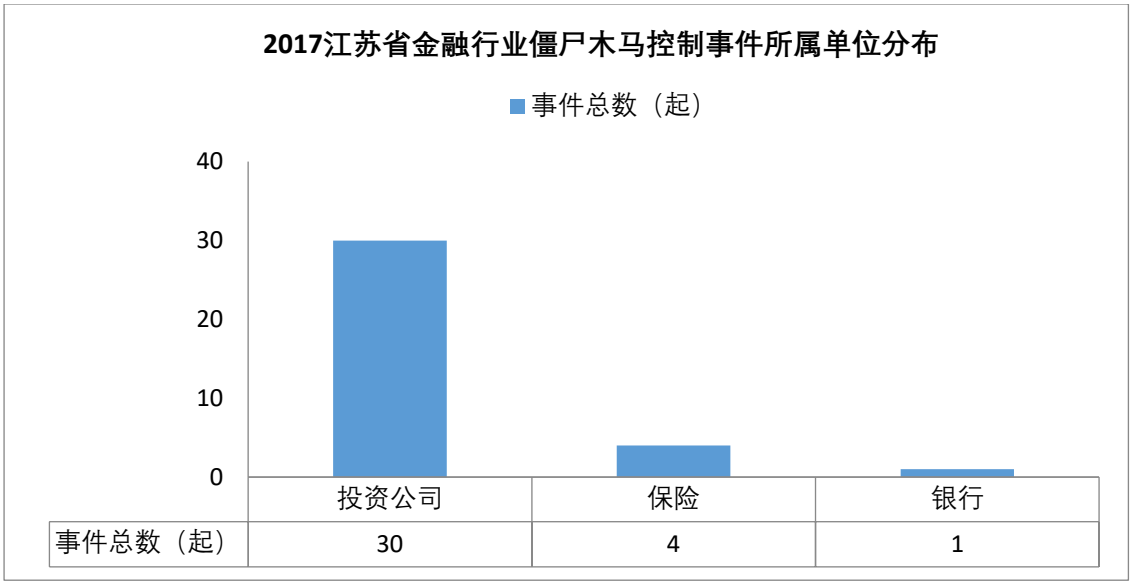


图 7.14 2017 年江苏省金融部门僵尸木马控制事件所属单位分布图

感染僵尸木马病毒事件数量最多的金融部门为投资公司、银行、保险公司，其中投资公司感染事件数最多，达 48.65 万起。金融行业僵尸木马受控事件所属单位分布如图 7.15 所示。

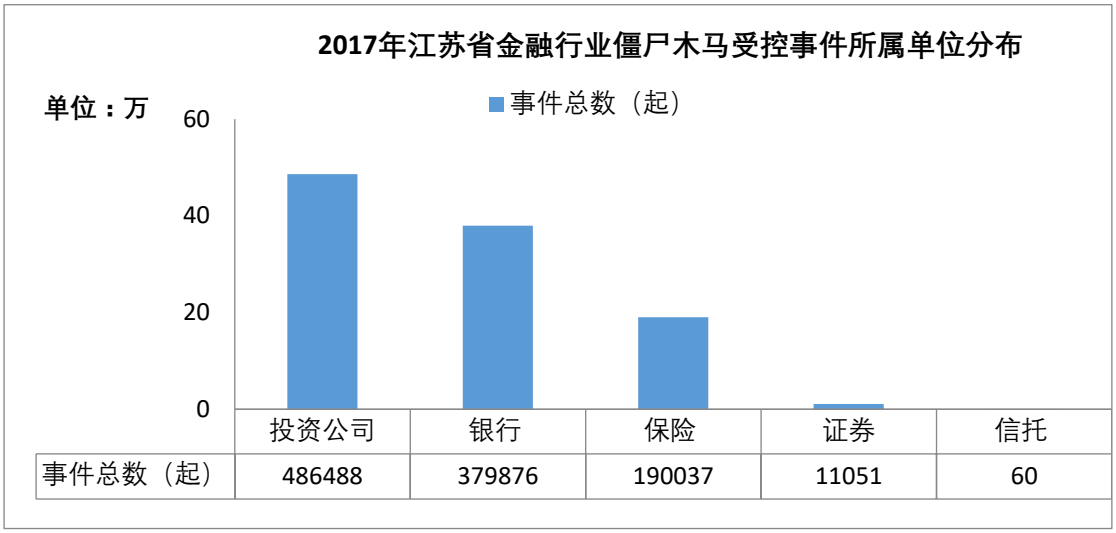


图 7.15 2017 年江苏省金融行业僵尸木马受控事件所属单位分布图

7.3 教育行业互联网安全状况

2017 年，江苏省教育行业发生的各类网络安全事件共 6086.46 万起，其中僵尸木马受控事件最多，达 6071.01 万起，占事件总数的 99.75%。江苏省高校间接成为网络攻击源，是江苏省网络安全监管的短板。高校网络安全事件分布如图 7.17 所示。

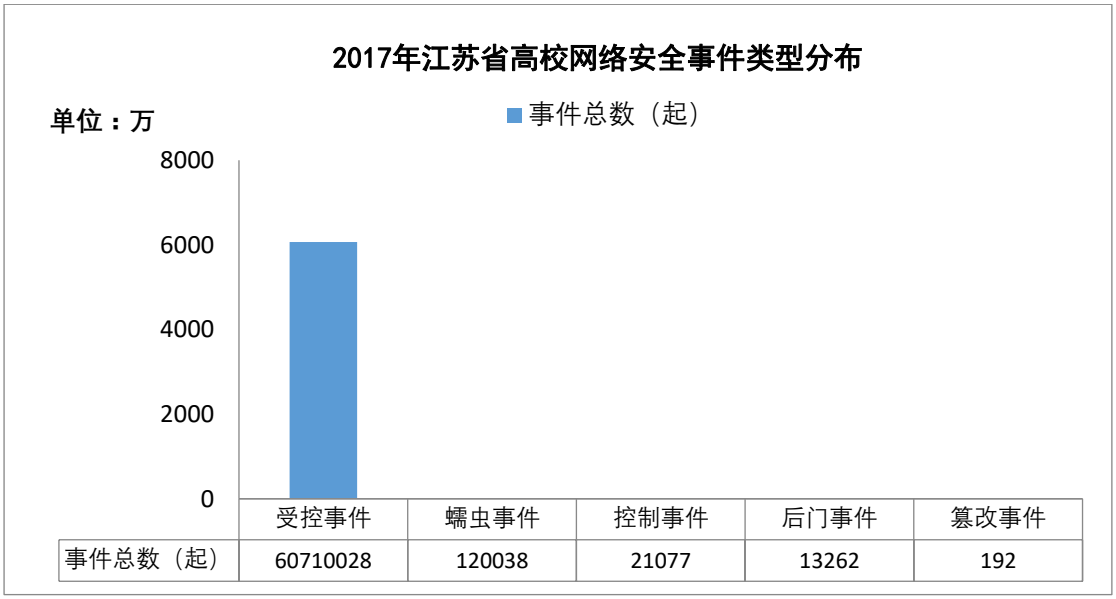


图 7.17 2017 年江苏省高校网络安全事件所属类型分布图

8、2017年网安热点及CNCERT/JS重点工作

8.1 国际国内热点问题

8.1.1 《中华人民共和国网络安全法》正式实施

2017年6月1日，《中华人民共和国网络安全法》正式实施。这是我国互联网领域的基础性法律，其中明确规定要加强对个人信息的保护。另外，最高人民法院和最高人民检察院发布的相关法律解释也于当日实行，进一步明确了侵犯公民个人信息罪的定罪量刑标准。

《网络安全法》的公布和施行，不仅从法律上保障了广大人民群众在网络空间的利益，有效维护了国家网络空间主权和安全，而且还有利于信息技术的应用，有利于发挥互联网的巨大潜力。《网络安全法》进一步界定了关键信息基础设施范围；明确加强个人信息保护；对攻击、破坏我国关键信息基础设施的境外组织和个人规定相应的惩治措施；增加惩治网络诈骗等新型网络违法犯罪活动的规定等。

同期实行的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》，进一步明确了侵犯公民个人信息罪的定罪量刑标准。《解释》共十三条，包括明确了“公民个人信息”的范围、非法“提供公民个人信息”的认定标准等十个方面内容。

8.1.2 国内相继出台多项网络安全相关指导意见

6月27日，中央网络安全和信息化领导小组办公室印发《国家网络安全事件应急预案》，预案自印发之日起实施。11月23日，工业和信息化部印发《公共互联网网络安全突发事件应急预案》，预案自印发之日起实施。两项网络安全应急预案分别明确阐释了事件分级、监测预警、应急处置、预防与应急准备、保障措施等相关内容，对提高我国网络安全等级，有效应对网络安全事件，预防和减少网络安全事件造成的损失和危害，保护公众利益，维护国家安全、公共安全和社会秩序具有重要的指导意义。

9月14日，工业和信息化部制定印发《公共互联网网络安全威胁监测与处置办法》，对公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件进行监测处置，并建立网络安全威胁信息共享平台，形成合力维护网络安全。该办法的出台，对于完善我国网络安全威胁监测处置、数据保护、新技术新业务安全评估等政策，最大限度地消除安全隐患、制止攻击行为、避免危害发生具有重要意义。

8.1.3 勒索病毒席卷全球

5月12日，“WannaCry”勒索病毒在全球范围内爆发，本次事件波及150多个国家和地区、10多万的组织和机构以及30多万网民，损失总计高达500多亿人民币。包括医院、教育机构以及政府部门，都无一例外的遭受到了攻击。勒索病毒结合蠕虫的方式进行传播，是此次攻击事件大规模爆发的重要原因。

6月27日，一种名为“Petya”的新勒索病毒席卷了欧洲，多家大型跨国企业中招，包括美国联邦快递公司、英国WPP广告公司、俄罗斯石油公司和丹麦马士基航运有限公司。“Petya”的传播方式还利用了“影子经纪人”泄露出来的安全漏洞。

10月，新型勒索软件“坏兔子”利用新闻媒体网站弹出的Adobe Flash软件安装请求来渗透用户电脑，而那些新闻媒体网站已经被黑客入侵了。这轮勒索风潮主要冲击了俄罗斯，但有专家发现乌克兰、土耳其和德国也出现了受害者。

8.1.4 物联网僵尸网络迅速蔓延

2016年，因遭遇僵尸网络Mirai攻击，亚马逊、Spotify和Twitter等知名网站纷纷中招，结果美国半个互联网瘫痪。2017年8月，CDN和云服务提供商Akamai Technologies的研究表明，Mirai事实上更类似于一群群小规模的bot和C&C服务器，不断的攻击促成了DDoS商业化。

9月，安全人员发现一个针对物联网设备的新僵尸网络。该僵尸网络扩张速度惊人，很快就感染了超过两百万台设备，包括路由器、摄像头等，而中国是感染的重灾区。

因为物联网设备安全漏洞较多，所以利用物联网组成的僵尸网络日渐庞大，DDoS攻击数量猛增，并且商业化运作越来越明显。

8.1.5 维基解密美国中央情报局（CIA）绝密文件泄露事件

2017 年 3 月 7 日，维基解密（WiKiLeaks）公布了数千份文档并揭秘了 CIA 关于黑客入侵技术的最高机密，根据泄密文档中记录的内容，该组织不仅能够入侵 iPhone 手机、Android 手机和智能电视，而且还可以入侵攻击 Windows、Mac 和 Linux 操作系统，甚至可以控制智能汽车发起暗杀活动。外界将此次泄漏事件取名为 Vault 7，Vault 7 公布的机密文件记录的是 CIA 所进行的全球性黑客攻击活动。

Vault7 包含 8761 份机密文件，这些文件记录了 CIA 针对 Android 以及 iPhone 智能手机所研发的入侵破解技术细节，其中有些技术还可以拿到目标设备的完整控制权。维基解密创始人阿桑奇表示，文件显示出“CIA 网络攻击的整体能力”，而维基解密在发布这些文件时声称“CIA 的网络军械库已失控”。

8.1.6 影子经纪人公开美国国家安全局（NSA）黑客武器库

2017 年 4 月，影子经纪人公开了一大批 NSA“方程式组织” (Equation Group)极具破坏力的黑客工具，其中包括可以远程攻破全球约 70% Windows 机器的漏洞利用工具。任何人都可以使用 NSA 的黑客武器攻击别人电脑。其中，有十款工具最容易影响 Windows 个人用户，包括永恒之蓝、永恒王者、永恒浪漫、永恒协作、翡翠纤维、古怪地鼠、爱斯基摩卷、文雅学者、日食之翼和尊重审查。黑客无需任何操作，只要联网就可以入侵电脑，就像冲击波、震荡波等著名蠕虫一样可以瞬间血洗互联网；5 月，影子经纪人宣称将从 6 月开始，向付费用户提供更多窃取自 NSA 的黑客工具和数据；6 月，影子经纪人推出月度服务，开始逐月出售包括浏览器、路由器、手机漏洞以及 SWIFT 供应商和央行的入侵数据，并于 7 月份向客户出售一批新的被盗代码，而购买这些代码的客户需要支付不低于 2.2 万美元的酬金；9 月 6 日，影子经纪人发消息宣布数据服务将调整为每月披露两批 NSA 网络武器，要价近 400 万美元；10 月 16 日，影子经纪人再发消息宣布服务价格的调整情况：所有数据转储内容以 500 ZEC 的价格出售。

8.2 2017 年 CNCERT/JS 重点工作

8.2.1 举办 2017（第五届）江苏互联网大会

以“聚力数字新经济 共建网络新空间”为主题的 2017（第五届）江苏互联网大会 9 月 26 日在南京举行。工业和信息化部副部长陈肇雄、江苏省副省长马秋

林出席大会并致辞。本届大会由省网信办、省通信管理局指导，省互联网应急中心、省互联网协会主办，大会参会人数逾3000人。

陈肇雄表示，党的十八大以来，以习近平同志为核心的党中央高度重视网络安全和信息化工作，做出了建设网络强国的重大战略部署。互联网作为创新最活跃、渗透最广泛、影响最深远的领域，与实体经济加快融合，促进了供给侧结构性改革，推动了传统产业数字化、网络化、智能化发展，培育壮大了新模式、新应用、新产业。江苏处在“一带一路”的交汇点上，发展数字经济具有独特的区位优势、市场优势和坚实的网络基础、产业基础，潜力巨大、前景广阔。

马秋林指出，江苏省认真贯彻落实网络强国、“互联网+”行动等国家战略，深入推进互联网和制造业深度融合，加快发展互联网经济，大力促进互联网在经济社会各领域的广泛应用，取得了显著成效。全省通信行业将进一步加强未来网络、5G通信网、下一代广播电视网等关键技术攻关和基础设施布局。

会上，互联网协会理事长、南京邮电大学校长杨震介绍了全省互联网发展状况，中国工程院院士沈昌祥和中国社科院工业经济研究所副所长李海舰为大会作了主题演讲。本次大会期间，一大批互联网学术界、企业界有重要影响力的知名学者和领军人物齐聚南京，立足江苏通信与互联网领域的发展特色，围绕数字经济和网络空间，共话互联网。大会设有“互联网助推江苏特色小镇建设”、“网络信息基础设施建设”、“互联网+新技术”、“互联网+共享经济”、“互联网+产业基金”、“网络安全”、“智慧生活”七个高峰论坛。

8.2.2 举办2017年度江苏省网络安全技能竞赛

2017年11月24日，由省总工会、省人社厅主办，省委网信办、省通信管理局、省互联网应急中心承办的2017年度江苏省网络安全技能竞赛圆满落下帷幕，颁奖仪式在江苏软件园成功举办。

江苏网络安全技能竞赛自2013年启动以来，受到了广泛关注。全省近500名从事网络安全相关职业的一线职工参加了本届大赛选拔赛。11月6日至10日，来自国家互联网应急中心、江苏省互联网应急中心、南京邮电大学、长亭科技等单位的11名网络安全专家为近百名安全技术人员进行现场培训。竞赛组委会技术组与国家互联网应急中心、省内外知名互联网公司以及网络安全企业合作，

选取了 10 名专家进行赛题筹备，形成理论和实操两部分试题，重点考核选手在安全渗透、代码审计、逆向分析、取证溯源等 23 个方面的网络安全技能。

各代表队在经过理论测试和实际操作的紧张角逐后，一批优胜团队和个人脱颖而出。其中获得个人赛前六名的选手现场被授予“江苏省五一创新能手”、“江苏省技术能手”称号；获得第一名的选手，经综合考察合格后，将按程序推荐申报“江苏省五一劳动奖章”。省总工会、省人社厅、省委网信办、省通信管理局等办赛单位领导及其他受邀嘉宾出席颁奖仪式，并为获奖的优秀团体和个人颁奖。

省通信管理局党组书记、局长袁瑞青作总结发言，对在竞赛中取得优异成绩的单位和选手表示祝贺，对指导帮助竞赛的部门表示感谢。他充分肯定了本次竞赛在培养、发现人才方面的成效，并号召各方共同努力，不断提高竞赛的吸引力和权威性，进一步把竞赛打造成江苏省乃至全国网络安全竞赛的知名品牌。同时，省通信管理局将认真贯彻落实《网络安全法》，加大政策指导和支持力度，建立适应行业特点的网络安全人才评价机制和激励机制，鼓励网络安全人才干事创业。

8.2.3 挂牌成立国家互联网应急中心江苏培训认证中心及苏州培训基地

为了进一步提升我省网络信息安全人才的数量和质量，优化完善人才队伍的结构与作用，探索创新培训与认证模式，国家互联网应急中心、江苏省互联网应急中心、中国移动通信集团江苏有限公司三方联合成立江苏培训认证中心及苏州培训基地。2017 年 7 月 7 日，认证中心与培训基地正式挂牌成立，国家互联网应急中心黄澄清主任、省通信管理局袁瑞青局长、江苏省互联网应急中心王云飞主任出席。

互联网快速发展，网络安全是前提，网络空间的竞争，归根到底是人的较量，队伍是基础，人才是关键。“聚天下英才而用之，为网信事业发展提供有力人才支撑”，在网络安全和信息化工作座谈会上，习近平总书记强调的人才观，为网信事业发展开阔了视野、指明了方向。

自 2013 年以来，在省总工会、省人社厅、省通信管理局的指导下，江苏省互联网应急中心连续四年承办江苏省网络安全技能竞赛，全省累计参加竞赛

2000人次，培育省五一劳模1人、省五一劳动奖章7人、设区市级五一劳动奖章126人。近年来，江苏网络安全人才再教育、再培训的市场也日趋成熟，具备了开展网络安全应急培训与认证的客观条件。通过整合国家互联网应急中心、江苏省互联网应急中心和中国移动通信集团三方优势资源，可以为我省信息通信以及各行业技术人才提供高质量、权威性的安全培训认证，为国家网络安全与信息化发展保驾护航。

8.2.4 开展跨地区移动互联网网络安全应急演练

为进一步提升江苏通信业应对突发网络信息安全事件的响应能力和协调处置能力，8月15日，在工业和信息化部网络安全管理局指导、福建省通信管理局协调下，江苏省通信管理局会同浙江省通信管理局，组织江苏省互联网应急中心、江苏电信、江苏移动、江苏联通，开展了以移动互联网安全事件为主题的跨地区网络安全应急演练。

本次演练分为四个阶段，分别为发现感染情况、分析研判、应急处置和反馈确认。针对传播较广、危害较为严重的“A.Privacy.htmlapp.j”移动互联网恶意程序，按照《江苏省公共互联网网络安全应急预案》，启动三级应急处理方案，通过溯源分析发现该恶意程序的源IP地址分别属于江苏电信、江苏移动、江苏联通和浙江，江苏省互联网应急中心协调相关方面对相关IP地址进行封堵处置，并通知用户做好服务器安全防护，完成了封堵验证。

本次演练成功实现了江苏电信、江苏移动、江苏联通、浙江省通信管理局等多家单位跨网的联动处置，充分检验了各参演单位应对突发安全事件的应急响应能力和协调处置能力，得到了工信部网络安全管理局相关领导的充分肯定；为进一步提升通信行业整体安全防护水平和应急处置能力，全面保障党的十九大、金砖峰会等重大活动打下了坚实基础。

8.2.5 推进全省重要信息系统网络安全事件监测处置

2017年，江苏省互联网应急中心联合省委网信办、省人民政府办公厅电子政务办公室、省保监局、中国人民银行南京分行、各设区市通信行业管理办公室等单位，以多种形式向各级党政机关、高校、医院等单位及关键信息基础设施运营单位发函通报网络安全事件，全年发布信息系统含有高危漏洞的预警通报函文354份，涉及漏洞799个，收到感谢函或复函453份。在与多部门联合

开展工作的基础上，江苏省互联网应急中心进一步拓展合作渠道，截至2017年底，已与盐城市城南新区、江苏省电化教育馆等60家单位建立了网络安全合作机制。

8.2.6 多渠道发布各类网络安全报告、预警

2017年，江苏省互联网应急中心定期发布安全通报，全年向省委省政府主要领导及省内部分委办厅局报送《江苏省互联网网络安全专报》12期，向省内基础通信运营企业及大型互联网增值企业下发《江苏省互联网网络安全信息通报》12期，向社会公众发布《江苏省互联网网络安全月报》12期，向省内基础通信运营企业及各支撑单位转发国家互联网应急中心各类通报及预警428份，指导全省各设区市通信行业管理办公室、互联网协会编写《互联网网络安全专报》，所有报送单位达137家。此外，江苏省互联网应急中心还通过门户网站、中国江苏网、微信公众号、微博等多种渠道发布网络安全事件及预警信息。

8.2.7 正式启用江苏省互联网应急中心综合机房楼

2017年7月7日，江苏省互联网应急中心综合机房楼正式启用。参加启用仪式的领导有国家互联网应急中心主任黄澄清、江苏省通信管理局局长袁瑞青、南京市副市长华静、建邺区区长闵一峰、建邺区常务副区长李方毅等。江苏省互联网应急中心主任王云飞主持启用仪式。

启用仪式上，袁瑞青局长指出，综合机房楼的建成为江苏省互联网应急中心实现更高层次的发展创造了更好的硬件环境，希望江苏省互联网应急中心全力做好各类保障，同时继续做好机房楼配套建设和物业等规范管理工作。华静副市长表示，南京市政府将竭尽全力、积极支持江苏省互联网应急中心开展工作，为实现“强富美高”新南京做出更大贡献。黄澄清主任认为，江苏省互联网应急中心综合机房楼项目将为今后各项工作的开展提供更强有力的保障，对于进一步提升江苏省网络信息安全保障水平、促进本省经济发展和维护社会安全稳定具有重要意义。

8.3 江苏省网络安全组织发展情况介绍

8.3.1 江苏省网络安全应急支撑单位

互联网作为重要信息基础设施的桥梁，社会功能日益增强，但由于本身的开放性和复杂性，互联网面临巨大的安全风险，因此，面向公共互联网的应急处置工作逐步成为公共应急服务事业的重要组成部分，建立高效的公共互联网应急体系和强大的人才队伍，对及时有效地应对互联网突发事件有着重要意义。为拓宽掌握互联网宏观网络安全状况和网络安全事件信息的渠道，增强对重大突发网络安全事件的应对能力，强化公共互联网网络安全应急技术体系建设，促进互联网网络安全应急服务的规范化和本地化，经工业和信息化部批准，2004 年 CNCERT/CC 首次面向社会公开选拔了一批国家级、省级公共互联网应急服务试点单位。经过多年发展，应急服务支撑单位已成为我国公共互联网网络安全应急体系的重要组成部分，强化我国公共互联网网络安全技术体系建设，促进我国互联网网络安全预警发现和应急响应能力，维护我国互联网网络安全，国家重大活动期间保障网络安全发挥了重要作用。每两年，CNCERT/CC 会组织开展网络安全应急服务支撑单位选拔工作，网络安全应急服务支撑单位由各省进行推荐上报。2017 年，最终评选出 10 个国家级和 51 个省级网络安全应急服务支撑单位，其中由江苏省互联网应急中心推荐的有 10 个国家级和 10 个省级网络安全应急服务支撑单位。

江苏省网络安全应急服务支撑单位见表 8-1（有效时限为 2017 年 5 月 24 日至 2019 年 6 月 10 日）

表 8-1　江苏省网络安全应急服务支撑单位列表（排名不分先后）

单位名称	级别	证书编号
北京安天网络安全技术有限公司	国家级	CNCERT-2017-190524GJ001
恒安嘉新（北京）科技股份公司	国家级	CNCERT-2017-190524GJ002
网神信息技术（北京）股份有限公司	国家级	CNCERT-2017-190524GJ003
北京神州绿盟科技有限公司	国家级	CNCERT-2017-190524GJ004
深信服科技股份有限公司	国家级	CNCERT-2017-190524GJ005
北京天融信网络安全技术有限公司	国家级	CNCERT-2017-190524GJ006
北京启明星辰信息安全技术有限公司	国家级	CNCERT-2017-190524GJ007
长安通信科技有限责任公司	国家级	CNCERT-2017-190524GJ008
杭州安恒信息技术股份有限公司	国家级	CNCERT-2017-180524GJ001
沈阳东软系统集成工程有限公司	国家级	CNCERT-2017-180524GJ002
中国电信集团系统集成有限责任公司	省级	CNCERT-2017-190524SJ001
南京铱迅信息技术股份有限公司	省级	CNCERT-2017-190524SJ002
任子行网络技术股份有限公司	省级	CNCERT-2017-190524SJ008
南京赛宁信息技术有限公司	省级	CNCERT-2017-190524SJ030

北京永信至诚科技股份有限公司	省级	CNCERT-2017-190524SJ031
江苏金盾检测技术有限公司	省级	CNCERT-2017-190524SJ036
江苏君立华域信息安全技术股份有限公司	省级	CNCERT-2017-190524SJ037
北京数字观星科技有限公司	省级	CNCERT-2017-190524SJ042
江苏省邮电规划设计院有限责任公司	省级	CNCERT-2017-190524SJ044
江苏天创科技有限公司	省级	CNCERT-2017-190524SJ045

8.3.2 江苏省网络安全信息通报成员单位

江苏省互联网应急中心作为通信行业网络安全信息通报中心，积极贯彻落实工业和信息化部颁布的《互联网网络安全信息通报实施办法》，协调和组织各设区市通信行业管理办公室、基础电信企业、增值电信业务经营企业以及安全企业开展通信行业网络安全信息通报工作。江苏省互联网应急中心积极拓展信息通报工作成员单位，并努力规范各通报成员单位报送的数据。截至2017年12月，共吸纳50家信息通报工作成员单位，形成较稳定的信息通报工作体系。全省50家信息通报工作成员单位情况见表8-2。

表8-2 通信行业互联网网络安全信息通报工作单位（排名不分先后）

各设区市通信行业管理办公室（13家）	全省各设区市通信行业管理办公室
基础电信运营基础通信运营企业（4家）	中国电信股份有限公司江苏分公司
	中国移动通信集团江苏有限公司
	中国联合网络通信有限公司江苏省分公司
	中移铁通有限公司江苏分公司
科研院所（1家）	全球能源互联网研究院
网安及增值企业（32家）	中国电信集团系统集成有限责任公司
	联通系统集成有限公司江苏省分公司
	江苏省邮电规划设计院有限责任公司
	北京奇虎360科技有限公司
	北京瑞星信息技术有限公司
	北京启明星辰信息安全技术有限公司
	北京神州绿盟信息安全科技股份有限公司
	北京天融信网络安全技术有限公司
	深圳市深信服电子科技有限公司
	北京知道创宇信息技术有限公司
	亚信科技（成都）有限公司
	哈尔滨安天科技股份有限公司
	恒安嘉新（北京）科技有限公司
	杭州安恒信息技术有限公司
	江苏国瑞信安科技有限公司
	南京铱迅信息技术股份有限公司
	江苏天创科技有限公司
	东软集团股份有限公司

网安及增值企业（32 家）	江苏南谷云信息技术有限公司
	江苏君立华域信息安全技术股份有限公司
	南京太极网络通信有限公司
	东巽科技（南京）有限公司
	南京云嘉德信息科技有限公司
	江苏金盾检测技术有限公司
	南京慧必特信息科技有限公司
	网神信息技术（北京）股份有限公司
	江苏国保信息系统测评中心有限公司
	北京亚鸿世纪科技发展有限公司
	任子行网络技术股份有限公司
	北京数字观星科技有限责任公司
	南京英孚浩迈信息科技有限公司
	江苏全博信息科技有限公司

8.3.3 江苏省互联网协会通信网络安全专业委员会

本着团结业界各方人士，坚持以服务为宗旨，努力为通信安全行业服务，促进通信网络安全工作的改进与提高，推动通信安全服务市场的规范和有序运行，江苏省互联网应急中心于 2011 年在江苏省通信行业协会、江苏省互联网协会指导下，成立了江苏省互联网协会通信网络安全专业委员会；截止目前，共有 39 家成员单位，江苏省互联网应急中心连续两届担任主任委员单位。江苏省通信网络安全专业委员会会员单位情况见表 8-3。

表 8-3　江苏省通信网络安全专业委员会会员单位（排名不分先后）

主任会员单位	江苏省互联网应急中心
副主任会员单位	中国电信股份有限公司江苏分公司
	中国移动通信集团江苏有限公司
	中国联合网络通信有限公司江苏省分公司
	深圳市深信服电子科技有限公司
	北京天融信网络安全技术有限公司南京分公司
	曙光信息产业股份有限公司江苏分公司
	江苏国瑞信安科技有限公司
	南京太极网络通信有限公司
	南京南谷云信息技术有限公司
会员单位	中移铁通集团有限公司江苏分公司 全球能源互联网研究院
	江苏有线数据网络有限责任公司
	江苏省邮电规划设计院有限责任公司
	北京启明星辰信息安全技术有限公司
	北京神州绿盟信息安全科技股份有限公司上海分公司
	焦点科技股份有限公司

会员单位	江苏三六五网络股份有限公司
	北京瑞星信息技术有限公司
	亚信科技（成都）有限公司
	杭州安恒信息技术有限公司
	恒安嘉新（北京）科技有限公司
	南京铱迅信息技术股份有限公司
	北京亚鸿世纪科技发展有限公司
	东软集团股份有限公司南京分公司
	江苏天创科技有限公司
	江苏君立华域信息安全技术股份有限公司
	东巽科技（南京）有限公司
	常州贝特康姆软件技术有限公司
	扬州欧普汇融软件技术有限公司
	哈尔滨安天科技股份有限公司
	南京赛宁信息技术有限公司
	远江盛邦（北京）网络安全科技股份有限公司
	南京安尊信息科技有限公司
	江苏快页信息技术有限公司
	上海犇众信息技术有限公司
	南京奥尔特信息科技有限公司

9、2017 年网络安全态势分析及 2018 年趋势预测

9.1 2017 年网络安全态势分析

9.1.1 我国网络安全法律法规日趋完善

《中华人民共和国网络安全法》于 2017 年 6 月 1 日正式施行，作为我国网络安全领域的基础性法律，《网络安全法》在网络安全历史上具有里程碑意义，一直备受各界关注。《网络安全法》的公布和施行，不仅从法律上保障了广大人民群众在网络空间的利益，有效维护了国家网络空间主权和安全，还有利于信息技术的应用，有利于发挥互联网的巨大潜力。

作为我国网络安全领域的首部基础性和综合性保障法，《网络安全法》预留了诸多配套制度的接口，有待相关配套法规的进一步细化，以提高可操作性。自颁布以来，相关战略、配套法律法规及标准也相继出台或列入制定规划。在网络安全战略层面，相继颁布国家和国际网络空间安全战略，提出我国参与网络空间治理的战略任务和行动计划；在法律法规层面，国家各主管单位也从关键信息基础设施、个人信息和重要数据出境、网络安全事件、网络产品和服务的安全审查、互联网信息内容治理、网络安全学院建设、网络关键设备和专用产品等方面入手，进行了有针对性的规定，为《网络安全法》的遵从和执行提供切实依据；在强制性配套标准方面，全国信息安全标准化技术委员会 2017 年为落实《网络安全法》要求，加快推动重点标准研制，包括网络安全产品与服务、关键信息基础设施保护、网络安全等级保护等强制性国家标准的研究。

9.1.2 工业互联网安全防护得到高度重视

党的十九大报告提出“推动新型工业化、信息化、城镇化、农业现代化同步发展”“加快建设制造强国，加快发展先进制造业，推动互联网、大数据、人工智能和实体经济深度融合”。

近年来，乌克兰连续发生黑客攻击导致大面积断电事件。美国 2017 年举行的“网络卫士”年度例行网络安全演习，以及今年“网络风暴”演习重点都是工业

基础设施。2017 年发生的“永恒之蓝”勒索病毒事件利用了美国泄漏的网络武器，是网络战的一次预演，造成我国众多工业企业中招，占各行业被攻击总数的17.3%，给经济社会带来严重影响。

2017 年，国务院适时下发了《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》，分别从企业、行业、国家三个层面明确提出了安全技术手段建设任务。企业层面，要求相关企业落实网络安全主体责任，加大安全投入，通过加强技术手段建设提升自身安全防护能力，开展工业互联网安全试点示范；行业层面，支持相关产业联盟积极发挥引导作用，整合行业资源，创新安全服务模式，提升行业整体安全保障服务能力；国家层面，充分发挥国家专业机构和社会力量的作用，增强国家级工业互联网安全技术支撑能力，着力提升隐患排查、攻击发现、应急处置和攻击溯源能力。

9.1.3 网络攻击军火化，网络武器民用化

2017 年，我们面对多种多样的网络攻击，安全危机进一步加剧。“WannaCry”、“Petya”、“BadRabbit”勒索病毒连续爆发，不断挑战着我们的网络安全防线。受勒索病毒影响，国内诸多企事业单位、高校的网站、应用系统和数据文件被加密，国外还影响到部分国家关键信息基础设施的正常运转。据腾讯监测统计，2017 全年总计检测敲诈勒索病毒样本数量在 660 万个，平均每月检测到敲诈勒索病毒数量近 55 万个。

而 2017 年 4 月，“影子经纪人”对外公布的网络攻击“核武器”工具包括网页浏览器、路由器和手机的安全漏洞及利用工具，微软“Windows10”操作系统安全漏洞；数据则包括 NSA 入侵环球银行间金融通信协会(SWIFT)和一些国家中央银行系统所盗取的网络数据，入侵俄罗斯、伊朗和朝鲜等国的核及导弹计划系统所盗取的网络数据等。

有专家认为：勒索病毒的大规模爆发会成为一个里程碑事件，“高危漏洞+网络武器”会成为标配，这些“核武器”将会变成研究重点。

9.1.4 安全漏洞数量激增，固件和协议漏洞频发

根据国家信息安全漏洞共享平台（CNVD）统计，2017 年共计收录 15955 个安全漏洞，环比增长 47.43%，其中，中高危漏洞所占比例已逾九成。5 月，Intel 公司公布了一个严重高危级别安全漏洞，攻击者可以在目标操作系统不可

直接访问的区域进行加载/执行任意代码的操作，具备极高的隐蔽性，常规方法无法检测到；7月，博通 WiFi 芯片也被披露存在“Broadpwn”远程代码执行漏洞，影响 Android 和 iOS 数十亿台设备；10 月，针对 WiFi+WPA2 网络，名为 KRACK 的漏洞攻击方式被披露，影响包括 Linux、Android、Cisco wireless products、OpenBSD、MacOS、Windows、iOS 等众多产品或平台。上述部分高危漏洞厂家或许能够及时提供解决方案，但是协议漏洞动辄影响上亿台的设备，而协议的更新换代则需要漫长的时间周期，甚至像部分固件漏洞永远难以修复，现实中诸多老旧系统和设备的安全漏洞也将是最大的挑战。

9.1.5 虚拟货币成为网络违法犯罪的帮凶

2017 年，随着“炒币”行为越来越热门，基于区块链技术的虚拟币不断涌现。虚拟货币的火热同时也引起了全世界黑客的强烈关注，他们试图利用各种方法来牟取利益。主要包括两种，一种是利用勒索病毒直接向用户勒索，另一种是利用挖矿病毒让感染用户挖掘。

2017 年，“WannaCry”、“Petya”、“BadRabbit”勒索病毒连续爆发，受害人只有支付赎金，才能再次访问自己电脑上的数据。而所谓的赎金都是以虚拟货币结算，这也导致虚拟货币在 2017 年涨势疯狂，排在前十位的虚拟货币平均涨幅为 13839%，其中单一比特币从年初的不足 1000 美元最高涨至近 20000 美元。有专家就这样评论：勒索病毒不在乎冻结你电脑后要你的多少个比特币，他要的是让全世界知道比特币的作用，这是个赤裸裸的营销策划方案。

虚拟货币已日益成为各类违法犯罪活动的“帮凶”，潜藏巨大的社会风险。

9.1.6 人工智能（AI）成为网络安全行业热点

AI 应该是 2017 年互联网最热的词汇了，它已经站在科技浪头，在网络安全中的应用更是大势所趋。

目前，黑客已经开始利用人工智能进行网络攻击，不仅扩大了攻击面，也提升了攻击手段。面对利用人工智能进行的黑客攻击，我们的最佳防御策略也是利用人工智能。我们可以在海量数据中，通过 AI 去发现异常、捕获威胁，实现威胁与入侵的快速感知和响应，这是传统的单点安全防护所做不到的。理论和实践都表明，数据规模越大，维度越丰富，训练出来的 AI 模型的适应性就越

强。因此，汇总各部门、各行业的数据，利用 AI 技术进行挖掘和分析，及时发现网络安全威胁并有效应对。

9.2 2018 年网络安全趋势预测

9.2.1 移动端安全将成为网络攻防的主战场

Andriod 系统已连续多年位居产品漏洞数量榜首，成为名副其实的“漏洞之王”。手机、WiFi 已经成为现代人生活必不可少的因素，针对移动端的攻击越发普及，Android 的市场占有率已逾八成，使得黑产毫无迟疑的专注 Android 系统，Android 病毒将展现更多面的恶意行为，已经不光专注于短信拦截、隐私盗窃、恶意扣费等，黑产已经利用移动病毒为多种业务服务，比如利用宿主手机资源对应用商店中某款应用恶意刷量，后期 Android 用户将面临更大的安全风险。

9.2.2 区块链技术将蓬勃发展，文件加密勒索将更加猖獗

2017 年，让无数人知道了“勒索软件”一词，黑客利用暂时无解的加密方法对用户进行 “比特币”勒索。加之，2017 年比特币价格疯涨，猜想 2018 年黑客会继续利用系统及应用漏洞进行攻击，而且勒索软件的魔爪很有可能会伸向物联网设备、POS 机和自动取款机。回首 2017，不难发现，数字加密货币已成为了多起勒索病毒攻击事件支付赎金的方式，一定程度上数字加密货币成为了黑客攻击的罪源。鉴于区块链技术的快速发展，预测 2018 年，该技术将在更多领域得以应用，而由于数字加密货币的特殊性，由区块链技术催生的恶意攻击活动在 2018 年将更加频繁，相关安全形势将愈发严峻。

9.2.3 黑客将利用人工智能与机器学习技术发起攻击

2017 年，在讨论网络安全议题时，必然会讨论到人工智能和机器学习技术。然而，有关人工智能和机器学习的讨论都专注于如何将这些技术用于保护和监测。预计 2018 年，这种情况将发生变化，攻击者将会利用人工智能和机器学习发动攻击。我们将在网络安全领域看到人工智能攻防比拼的一年。攻击者将会使用人工智能发动攻击，并且用于探索受害者的网络，这通常是他们成功入侵受害者系统后最耗费精力的环节。而防护者将依托人工智能挖掘发现潜在的异常，帮助其及时有效的进行应对。

9.2.4 更多物联网设备将被 DDoS 攻击利用

2017 年，我们看到利用家庭和工作场所中成千上万的存在安全漏洞的物联网设备生成流量而发起的大型 DDoS 攻击。预计 2018 年，这种情况不会改善，攻击者仍会利用安全设置和管理措施不当的家庭物联网设备来发动攻击。此外，攻击者还会劫持设备的输入/传感器，然后通过音频、视频或其他伪造输入，让这些设备按照他们的期望而非用户的期望操作。

9.2.5 无文件和轻文件恶意软件爆发

2017 年，无文件（File-less）和轻文件（File-light）恶意软件不断增长，攻击者将目标瞄准防御措施较低的企业。由于较少的入侵指标（IoC）、受害者所使用的工具，以及他们复杂无章的行为，在很多情景下，这些威胁难以被阻止、跟踪和防御。类似于早期的勒索软件，当少数攻击者成功勒索后，这便激发了其他攻击者的兴趣。如同淘金热一般，现在更多攻击者正在争相使用这些相同的技术来发动攻击。虽然无文件和轻文件恶意软件与传统恶意软件不在一个数量级上，但也会构成巨大的威胁，导致这些恶意软件在 2018 年大爆发。

关于国家计算机网络与信息安全管理中心江苏分中心

国家计算机网络与信息安全管理中心江苏分中心（中文简称江苏省互联网应急中心，英文简称 CNCERT/JS）是国家计算机网络与信息安全管理中心（中文简称国家互联网应急中心，英文简称 CNCERT/CC，隶属中央网络安全和信息化委员会办公室管理）在江苏省的分支机构，受国家互联网应急中心垂直管理，是江苏省公共互联网网络安全事件的**“监测中心、通报中心、处置中心、技术支撑中心”**，通过已有应急体系和自身技术平台对江苏省公共互联网络相关的安全威胁进行常规和重点监测，并定期发布本省网络安全情况通报，为江苏省公共互联网、重要政府部门、通信运营企业、关键信息基础设施运营单位提供计算机网络安全的发现、预警、通报、处置等技术支撑。

主要能力包括：

✓事件监测：依托全程全网、多层次、多渠道延伸的网络安全综合发现平台，实现各类网络安全事件的发现分析。江苏省互联网应急中心目前已具备木马和僵尸网络[4]发现、网页篡改[5]发现、网页挂马[6]发现、网页仿冒[7]发现、恶意代码捕获、公共互联网网络流量异常发现、域名服务发现、移动互联网恶意程序发现等能力。

✓通报预警：依托对丰富数据资源的综合分析和多渠道的信息获取，实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等，承担江苏省互联网网络安全信息通报工作。

✓应急处置：依托与江苏省通信运营企业、关键信息基础设施运营单位、安全服务厂商等相关部门建立的快速协作机制，实现网络安全事件的应急处置；制定并发布江苏省公共互联网网络安全应急预案，不定期组织江苏省公共互联网网络安全应急演练。

✓技术支撑：依托国家互联网应急中心及各网络安全应急支撑单位的技术团队，实现对省内关键信息基础设施运营单位的网络安全技术支撑；分析、研

[4]木马：以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意代码；僵尸：用于构建僵尸网络以形成大规模攻击平台的恶意代码。

[5]网页篡改：恶意破坏或更改网站页面内容，使网站无法正常工作或出现黑客插入的非正常网站内容。

[6]网页挂马：通过在网页中嵌入恶意代码或链接，致使用户计算机在访问该页面时被植入恶意代码。

[7]网页仿冒：通过构造与某一目标网站高度相似的页面（俗称钓鱼网站），并通常以垃圾邮件、即时聊天、手机短信、虚假广告等方式诱骗用户访问钓鱼网站获取用户个人秘密信息。

判并处置针对关键信息基础设施运营单位的网络安全攻击事件；支撑重点单位重要时期的网络安全防护。

✓安全研究：持续跟踪研究互联网存在的各种网络安全问题和新兴技术，通过课题研究、网络安全应急演练等形式为网络安全事件的发现、应急处置提供技术参考和指引。

✓咨询培训：为江苏省政府部门、关键信息基础设施运营单位、重要企事业单位建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案提供咨询和培训。

✓安全服务：提供计算机网络安全事件监测、预警、处置服务，计算机网络与信息系统和产品检测服务，网络和系统风险评估服务，互联网舆情服务。

联系方式：

电邮：jscert@cert.org.cn

热线：025-85039883

网址：www.jscert.org.cn

微信号：江苏省互联网应急中心