《中国互联网站发展状况及其安全报告（2017）》——简版

第一部分 中国网站发展概况

2016 年，中国网站规模发展迅猛，互联网接入市场竞争激烈，市场集中度进一步提升，民营接入服务商发展成就显著，十强接入企业形成相对稳定的格局。中国网站在地域分布上呈现东部地区多、中西部地区少的发展格局，区域发展不协调、不平衡的问题仍为突出。中国网站主办者中单位举办网站仍为主流,2016 年占比进一步提高。2016 年随着新通用顶级域的迅速发展，网站主办者使用网站域名的选择性增多，但仍相对集中。中国互联网在“大众创业，万众创新”、“互联网+”等大环境下，行业创新创业更加活跃。

1.中国网站规模发展迅猛。

截至 2016 年 12 月底，中国网站总量达到 475.4 万个，同比年度净增长 48.7 万个，其中单位主办网站 367 万个、个人主办网站 108.4 万个。为中国网站提供互联网接入服务的接入服务商 1,212 家，网站主办者达到 364 万个，中国网站所使用的独立域名共计 645.7 万个，每个网站主办者平均举办网站 1.3 个，每个中国网站使用的独立域名平均 1.4 个。

2.互联网接入市场集中度进一步提升，十强接入企业形成相对稳定的格局。

一是互联网接入市场竞争日趋激烈。从事网站接入服务业务的市

场经营主体快速增长，2016 年全国新增已从事网站接入服务业务的市场经营主体 90 家。二是国退民进加剧,市场集中度进一步提升。三家基础电信企业直接接入的网站为中国网站总量的 5.2%，同比下降 0.9 个百分点；而接入网站数量排名前 20 的接入服务商接入网站数量占比由 2015 年底的 64.96%提高到 2016 年底的 70.8%，排名前 20 的接入服务商中只有一家基础电信企业省级公司，由 2015 年底排名第十五降至第十八；接入网站数量在 1 万以上的重点接入服务商数量比 2015 年增加 1 家为 53 家，53 家重点接入服务商接入网站总量为中国网站总量的 81.6%，比 2015 年提高 4.5 个百分点。三是接入市场差距初现端倪。2016 年单一接入服务商市场份额已超过 30%，2016 年底阿里云计算有限公司接入网站 160.6 万个，占全国接入商接入网站的 34.1%。四是接入网站数量排名前 10 的企业形成相对比较稳定的格局，这些企业均为民营接入服务商，民营接入服务商发展持续提升。

3.中国网站区域发展不协调、不平衡，区域内相对集中。

跟中国经济发展高度相似，中国网站在地域分布上呈现东部地区多、中西部地区少的发展格局，区域发展不协调、不平衡的问题较为突出。截止到 2016 年底，东部地区网站占比 68.3%，中部地区占比 18.5%，西部地区占比 13.2%。无论从网站主办者住所所在地统计，还是从接入服务商接入所在地统计，网站主要分布在广东、北京、江苏、上海、浙江、福建、山东等东部沿海省市；中部地区网站分布主要在河南、安徽和湖北，西部地区网站主要集中分布在四川、重庆和

陕西。

4.中国网站主办者中单位举办网站所占比例进一步提高。

在 475.4 万个网站中，网站主办者为“单位”举办的网站达到 367 万个，占中国网站总量的 77.2%，同比提高 13.4%。其中“企业”举办网站达到 344.3 万个，较 2015 年底增长 42.4 万个。主办者性质为“个人”的网站 108.4 万个，较 2015 年底增长 5.3 万个，主办者性质为“事业单位”、“政府机关”、“社会团体”的网站较 2015 年底分别出现小幅增长。中国网站主办者组成情况见图 1-1。

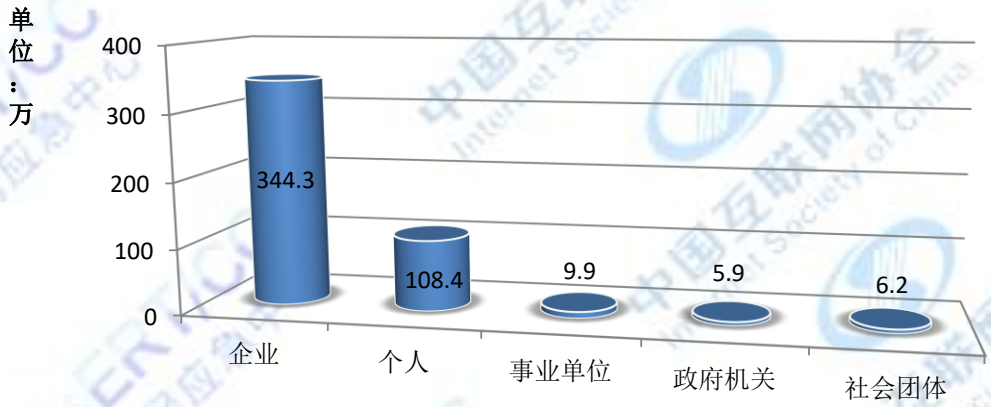


图 1-1：截至 2016 年 12 月底中国网站主办者组成情况

数据来源：中国互联网协会 2016.12

5.“.cn”、“.com”、“.net”仍为中国网站主办者使用的主流域名。

在中国网站注册使用的 645.7 万个独立域名中，注册使用“.cn”、“.com”、“.net”域名的中国网站数量仍最多，“.cn”、“.com”、“.net”独立域名使用数量占整个独立域名总量的 92.6%。截至 2016 年 12 月底，“.com”域名使用数量最多，达到 392 万个，其次为“.cn”和“.net”域名，各使用 171.2 万个和 34.4 万个，较 2015 年底分别增长 42、

24.3 和 1.4 万个。中国网站注册使用各类顶级域使用情况如图 1-2 所示。

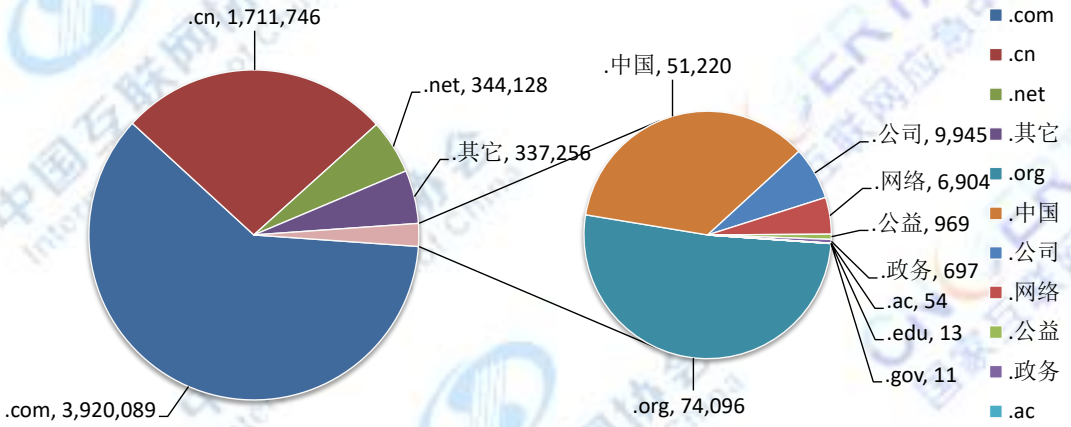


图 1-2：截至 2016 年 12 月底中国网站注册使用的各类顶级域占比情况

数据来源：中国互联网协会 2016.12

6. 中国网站注册使用新通用顶级域和中文域名的积极性显著提高。

截至 2016 年 12 月底，“.中国”、“.公司”、“.网络”等 25 类中文顶级域名达到 7.8 万个。2016 年全年中文域名总量使用情况如图 1-3 所示。

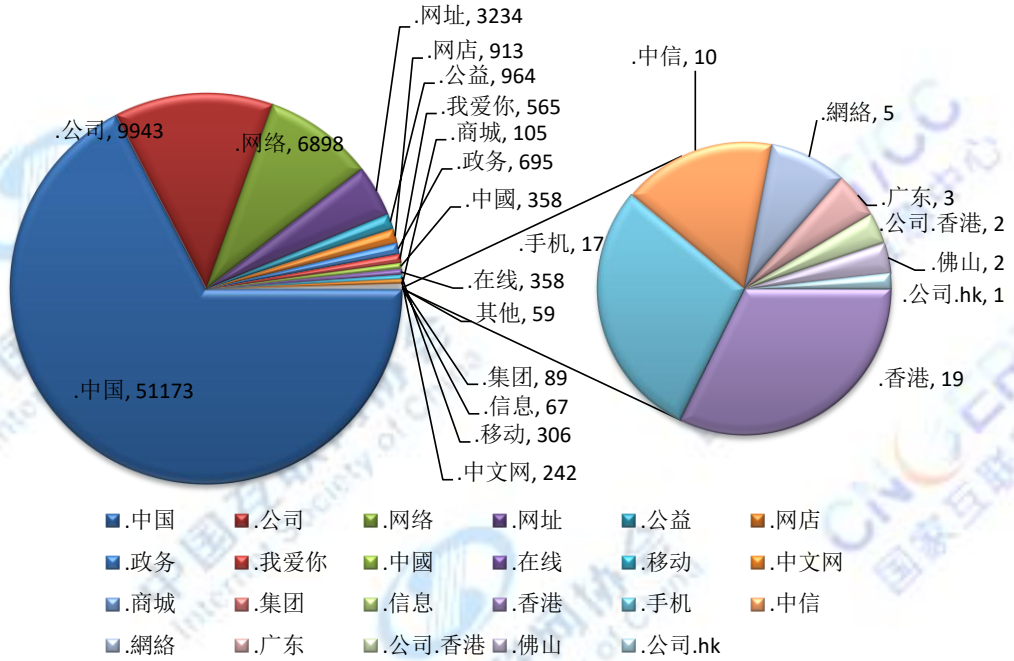


图 1-3：2016 年全年中文域名总量使用情况

数据来源：中国互联网协会 2016.12

随着新通用顶级域开放注册以来，公众对新通用顶级域的认知不断增长，2016 年新顶级域使用量明显增长，截止 2016 年底，“.wang”、“.ren”、“.网址”、“.xin”、“.xyz”等多个新通用顶级域的使用情况百分比如图 1-4。

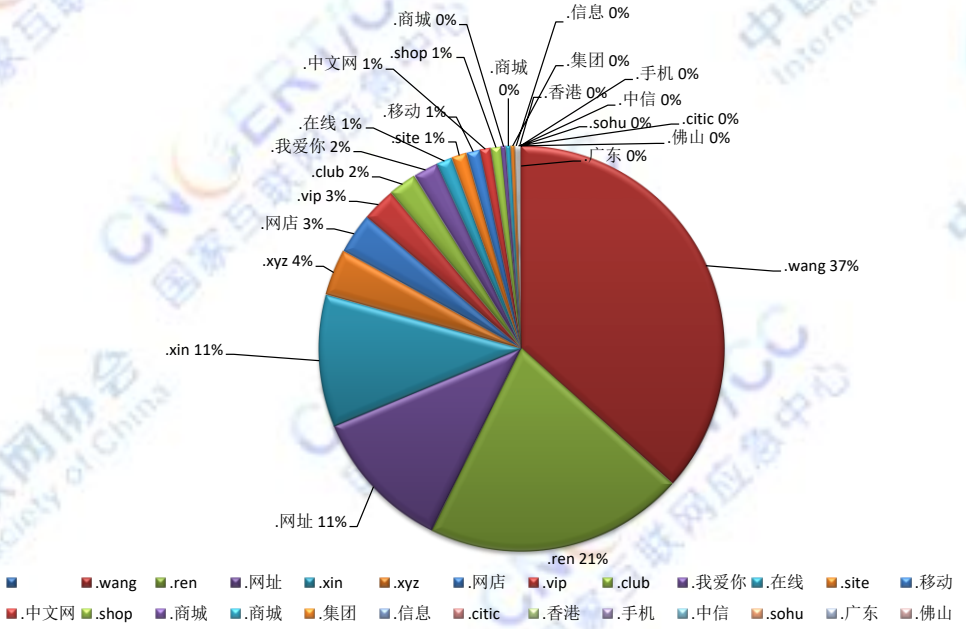


图 1-4：截至 2016 年 12 月底“.wang”、“.ren”等新通用顶级域使用情况百分比

7.中国网站语种呈多元化发展趋势。

中国网站语言日益丰富。截至2016年12月底，中国网站中除简体中文、繁体中文和英语之外，使用其他语言网站的数量较2015年底增长3,037个，其中包含法语、藏语、维吾尔语、蒙古语、哈萨克语、柯尔克孜语、西班牙语、日语、俄罗斯语等14种语言，多语言网站的持续增长,体现了中国网站内容和受众的多样性和广泛性，有力地支撑了中国人民的对外友好交往和中国改革开放的伟大事业。

8.中国互联网在“大众创业，万众创新”、“互联网+”等大环境下，行业创新创业更加活跃与频繁。

在国家大力实施创新驱动发展战略和“互联网+”行动计划的带领下，互联网领域呈现出前所未有的创业创新热情和氛围，互联网领域的创业创新正在引领新一轮科技革命和产业变革，2016年8月，中国互联网协会、工业和信息化部信息中心在京联合发布2016年“中国互联网企业100强”排行榜（简称“2016互联网百强”）。阿里巴巴、腾讯、百度、京东、奇虎360、搜狐、网易、携程、唯品会、苏宁云商位列2016年中国互联网百强榜前十位，京东自2014年进入前十以来，继续站稳第四的位置，前十名中，唯品会、苏宁云商两家企业挤掉了之前新浪、搜房网，首次跻身前十。创业创新是否成功与网站生存周期关系密切，2016年全年新开通的中国网站数量125.9万个，平均每月新开通网站10.5万个；全年网站主办者自行停办的中国网站68.2万个，平均每月自行停办的网站5.7万个。经过激烈地市场

竞争和洗礼，在电商、搜索、社交、游戏、文学、旅游、安全等众多领域涌现出具有一定规模的互联网企业。2016 年网站主办者新开通及自行停办的中国网站数量月变化情况见图 1-6。

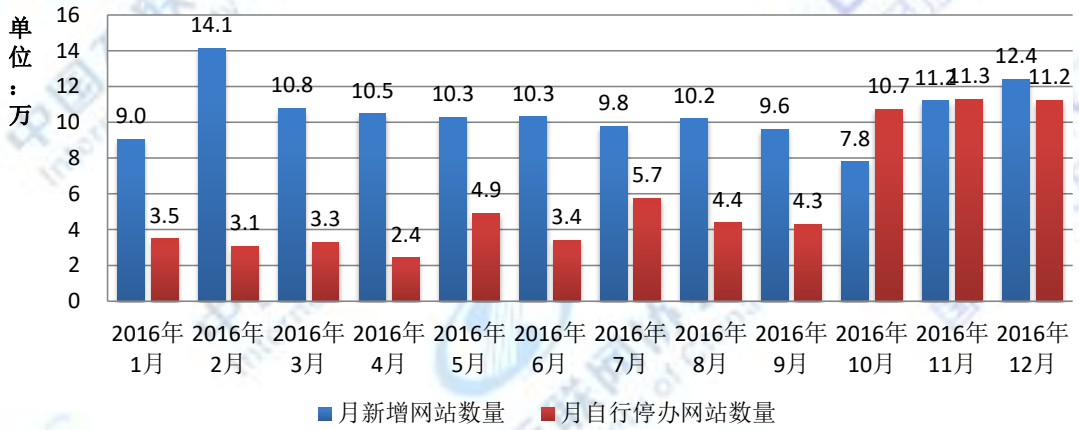


图 1-5：2016 年网站主办者新开通及自行停办的中国网站数量月变化情况

数据来源：中国互联网协会 2016.12

第二部分 中国网络安全总体态势情况

2016 年，是我国在网络空间法制化进程迈出实质性步伐的一年，《网络安全法》正式表决通过和《国家网络空间安全战略》正式发布进一步强化了我国网络安全顶层设计，为实现我国网络强国战略保驾护航。习近平总书记“419”等一系列讲话明确要求树立正确的网络安全观，为网络安全工作指明了主攻方向和行动理念。《中华人民共和国国民经济和社会发展第十三个五年规划纲要》（以下简称“十三五规划”）发布，明确提出实施网络强国战略，要求加快建设数

字中国，推动信息技术与经济社会发展深度融合，加快推动信息经济发展壮大。2016 年，作为“十三五规划”开局之年，网络经济空间发展大幅拓展趋势明显，推动信息技术服务向更为智能、与传统领域全面融合的阶段发展。然而，信息技术创新发展伴随的安全威胁与传统安全问题相互交织，使得网络空间安全问题日益复杂隐蔽，面临的网络安全风险不断加大，各种网络攻击事件层出不穷。

2016 年，我国互联网网络安全状况总体平稳，未出现影响互联网正常运行的重大网络安全事件，但移动互联网恶意程序数量持续高速上涨且具有明显趋利性；来自境外的针对我国境内的网站攻击事件频繁发生；联网智能设备被恶意控制，并用于发起大流量分布式拒绝服务攻击的现象更加严重；网站数据和个人信息泄露带来的危害不断扩大；欺诈勒索软件在互联网上肆虐；具有国家背景黑客组织发动的高级持续性威胁（APT）攻击事件直接威胁了国家安全和稳定。

国家互联网应急中心（以下简称“CNCERT”）在对我国互联网宏观安全态势监测的基础上，结合网络安全预警通报、应急处置工作实践成果，着重分析和总结了 2016 年我国互联网网络安全状况，总结如下七个突出的态势特点：

1.域名系统安全状况良好，防攻击能力明显上升

2016 年，我国域名服务系统安全状况良好，无重大安全事件发生。据抽样监测，2016 年针对我国域名系统的流量规

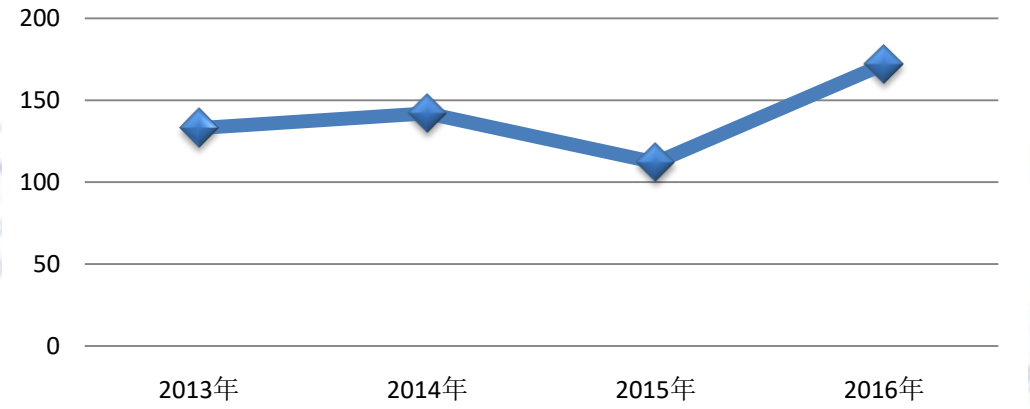
模达 1Gpbs 以上的 DDoS 攻击事件日均约 32 起，均未对我国域名解析服务造成影响，在基础电信企业侧也未发生严重影响解析成功率的攻击事件，主要与域名系统普遍加强安全防护措施，抗 DDoS 攻击能力显著提升相关。2016 年 6 月，发生针对全球根域名服务器及其镜像的大规模 DDoS 攻击，大部分根域名服务器受到不同程度的影响，位于我国的域名根镜像服务器也在同时段遭受大规模网络流量攻击。因应急处置及时，且根区顶级域缓存过期时间往往超过 1 天，此次攻击未对我国域名系统网络安全造成影响。

2. 针对工业控制系统的网络安全攻击日益增多

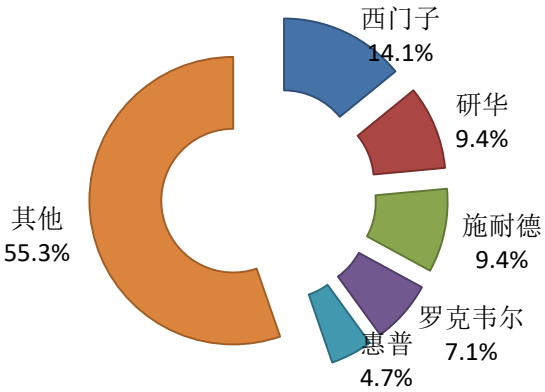
2016 年，全球发生的多起工控领域重大事件值得我国警醒。3 月，美国纽约鲍曼水坝的一个小型防洪控制系统遭攻击；8 月，卡巴斯基安全实验室揭露了针对工控行业的“食尸鬼”网络攻击活动，该攻击主要对中东和其他国家的工业企业发起定向网络入侵；12 月，乌克兰电网再一次经历了供电故障，据分析本次故障缘起恶意程序“黑暗势力”的变种。我国工控系统规模巨大，安全漏洞、恶意探测等均给我国工控系统带来一定安全隐患。截至 2016 年年底，CNVD 共收录工控漏洞 1036 条，其中 2016 年收录了 173 个，较 2015 年增长了 38.4%。工控系统主要存在缓冲区溢出、缺乏访问控制机制、弱口令、目录遍历等漏洞风险。同时，通过联网工控设备探测和工控协议流量监测，2016 年 CNCERT 共发

现我国联网工控设备 2504 个，协议主要涉及 S7Comm、Modbus、SNMP、EtherNetIP、Fox、FINS 等，厂商主要为西门子、罗克韦尔、施耐德、欧姆龙等。通过对网络流量分析发现，2016 年度 CNCERT 累计监测到联网工控设备指纹探测事件 88 万余次，并发现来自境外 60 个国家的 1610 个 IP 地址对我国联网工控设备进行了指纹探测。

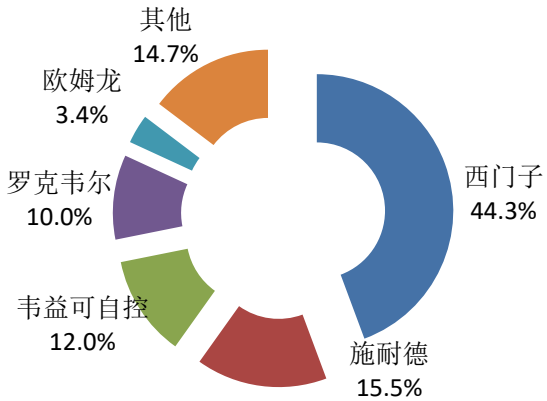
2013年至2016年CNVD收录工控系统漏洞情况



工控系统高危漏洞涉及厂商情况



发现的联网工控设备厂商分布情况



3. 高级持续性威胁常态化

截止到 2016 年底，国内企业发布高级持续性威胁（APT）研究报告共提及 43 个 APT 组织，其中针对我国境内目标发动攻击的 APT 组织有 36 个[1]。从攻击实现方式来看，更多 APT 攻击采用工程化实现，即依托商业攻击平台和互联网黑色产业链数据等成熟资源实现 APT 攻击。这类攻击不仅降低了发起 APT 攻击的技术和资源门槛，而且加大了受害方溯源分析的难度。2016 年，多起针对我国重要信息系统实施的 APT 攻击事件被曝光，包括“白象行动[2]”、“蔓灵花攻击行动”等，主要以我国教育、能源、军事和科研领域为主要攻击目标。2016 年 8 月，黑客组织“影子经纪人（Shadow Brokers）”公布了方程式组织[3]经常使用的工具包，包含各种防火墙的漏洞利用代码、黑客工具和脚本，涉及 Juniper、飞塔、思科、天融信、华为等厂商产品。CNCERT 对公布的 11 个产品漏洞（有 4 个疑似为 0day 漏洞）进行普查分析，发现全球有约 12 万个 IP 地址承载了相关产品的网络设备，其中我国境内 IP 地址有约 3.3 万个，占全部 IP 地址的 27.8%，对我国网络空间安全造成严重的潜在威胁。2016 年 11 月，黑客组织“影子经纪人”又公布一组曾受美国国家

[1]360 威胁情报中心发布的《2016 中国高级持续性威胁（APT）研究报告》。

[2]又名“摩诃草”黑客组织或“丰收行动”。

[3]方程式组织（Equation Group），世界上最尖端的网络攻击组织之一，疑似与美国国家安全局（NSA）有联系。

安全局网络攻击与控制的 IP 地址和域名数据，中国是被攻击最多的国家，涉及我国至少 9 所高校，12 家能源、航空、电信等重要信息系统部门和 2 个政府部门信息中心。

4. 大量联网智能设备遭恶意程序攻击形成僵尸网络

近年来，随着智能可穿戴设备、智能家居、智能路由器等终端设备和网络设备的迅速发展和普及利用，针对物联网智能设备的网络攻击事件比例呈上升趋势，攻击者利用物联网智能设备漏洞可获取设备控制权限，或用于用户信息数据窃取、网络流量劫持等其他黑客地下产业交易，或用于被控制形成大规模僵尸网络。CNCERT 对车联网系统安全性进行在线监测分析，发现部分车联网信息服务商及相关产品存在安全漏洞，可导致车辆、位置及车主信息泄露和车辆被远程控制等安全风险。2016 年底，因美国东海岸大规模断网事件和德国电信大量用户访问网络异常事件，Mirai 恶意程序受到广泛关注。Mirai 是一款典型的利用物联网智能设备漏洞进行入侵渗透以实现对设备控制的恶意代码，被控设备数量积累到一定程度将形成一个庞大的“僵尸网络”，称为“Mirai 僵尸网络”。又因物联网智能设备普遍是 24 小时在线，感染恶意程序后也不易被用户察觉，形成了“稳定”的攻击源。CNCERT 对 Mirai 僵尸网络进行抽样监测显示，截至 2016 年年底，共发现 2526 台控制服务器控制了 125.4 万余台物联

网智能设备，对互联网的稳定运行形成了严重的潜在安全威胁。此外，CNCERT 还对 Gafgyt 僵尸网络进行抽样检测分析，在 2016 年第四季度，共发现 817 台控制服务器控制了 42.5 万台物联网智能设备，累计发起超过 1.8 万次的 DDoS 攻击，其中峰值流量在 5Gpbs 以上的攻击次数高达 72 次。

5. 网站数据和个人信息泄露屡见不鲜，“衍生灾害”严重

由于互联网传统边界的消失，各种数据遍布终端、网络、手机和云上，加上互联网黑色产业链的利益驱动，数据泄露威胁日益加剧。2016 年，国内外网站数据和个人信息泄露事件频发，对政治、经济、社会的影响逐步加深，甚至个人生命安全也受到侵犯。在国外，美国大选候选人希拉里的邮件泄露，直接影响到美国大选的进程；雅虎两次账户信息泄露涉及约 15 亿的个人账户，致使美国电信运营商威瑞森 48 亿美元收购雅虎计划搁置甚至可能取消。在国内，我国免疫规划系统网络被恶意入侵，20 万儿童信息被窃取并在网上公开售卖；信息泄露导致精准诈骗案件频发，高考考生信息泄露间接夺去即将步入大学的女学生徐玉玉的生命；2016 年公安机关共侦破侵犯个人信息案件 1800 余起，查获各类公民个人信息 300 亿余条。此外，据新闻媒体报道，俄罗斯、墨西哥、土耳其、菲律宾、叙利亚、肯尼亚等多个国家政府的网站数据发生了泄漏。

6. 移动互联网恶意程序趋利性更加明确，移动互联网黑色产业链已经成熟

2016 年，CNCERT 通过自主捕获和厂商交换获得移动互联网恶意程序数量 205 万余个，较 2015 年增长 39.0%，近 6 年来持续保持高速增长趋势。通过恶意程序行为分析发现，以诱骗欺诈、恶意扣费、锁屏勒索等攫取经济利益为目的的应用程序骤增，占恶意程序总数的 59.6%，较 2015 年增长了近三倍。从恶意程序传播途径发现，诱骗欺诈行为的恶意程序主要通过短信、广告和网盘等特定传播渠道进行传播，感染用户数达到 2493 万人，造成重大经济损失。从恶意程序的攻击模式发现，通过短信方式传播窃取短信验证码的恶意程序数量占比较大，全年获得相关样本 10845 个，表现出制作简单、攻击模式固定、暴利等特点，移动互联网黑色产业链已经成熟。

7. 敲诈勒索软件肆虐，严重威胁本地数据和智能设备安全

根据 CNCERT 监测发现，2016 年在传统 PC 端，捕获敲诈勒索类恶意程序样本约 1.9 万个，数量创近年来新高。对敲诈勒索软件攻击对象分析发现，勒索软件已逐渐由针对个人终端设备延伸至企业用户，特别是针对高价值目标的勒索情况严重。针对企业用户方面，勒索软件利用安全漏洞发起攻击，对企业数据库进行加密勒索，2016 年底开源 MongoDB

数据库遭一轮勒索软件攻击，大量的用户受到影响。针对个人终端设备方面，敲诈勒索软件恶意行为在传统 PC 端和移动端表现出明显的不同特点：在传统 PC 端，主要通过“加密数据”进行勒索，即对用户电脑中的文件加密，胁迫用户购买解密密钥；在移动端，主要通过“加密设备”进行勒索，即远程锁住用户移动设备，使用户无法正常使用设备，并以此胁迫用户支付解锁费用。但从敲诈勒索软件传播方式来看，传统 PC 端和移动端表现出共性，主要是通过邮件、仿冒正常应用、QQ 群、网盘、贴吧、受害者等传播。