2017年我国互联网网络安全态势综述

国家计算机网络应急技术处理协调中心

2018年4月

目　录

前言

中国共产党第十九次全国代表大会胜利召开，大会报告提出，坚持和平发展道路，推动构建人类命运共同体，并指出网络安全是人类面临的许多共同挑战之一。党的十八大以来，以习近平同志为核心的党中央对网络安全工作做出了一系列重要的部署。2017 年 6 月 1 日，我国第一部《网络安全法》正式实施，我国网络安全管理迈入法治新阶段，我国网络空间法治体系建设加速开展。

党的十八大以来，我国确立了网络强国战略，加快数字中国建设，信息经济蓬勃发展，互联网成为国家发展的重要驱动力。截至 2017 年 12 月，我国网民规模达 7.72 亿，手机网民规模达 7.53 亿，互联网普及率达到 55.8%，超过全球平均水平和亚洲平均水平[①]。与此同时，2017 年,我国国内企业安全市场的整体规模约 400 亿元，同比增长约为 33%[②]。随着我国互联网普及和新技术、新业务的快速发展与应用，我国网络安全业务需求也在快速的增长。2017 年，在各方的共同努力下，我国网络安全防护和网络安全事件应急响应水平得到提升，网络安全国际合作进一步加强。但随着互联网应用的深化、网络空间战略地位的日益提升，网络空间已经成为国家或地区安全博弈的新战场，我国面临的安全问题日益复杂，敲诈勒索病毒盛行，分

[①]相关数据来源于中国互联网络信息中心发布的《第 41 次中国互联网络发展状况统计报告》。
[②]相关数据来源于中国互联网协会发布的《中国网络安全企业 50 强》（2017 年下半年）。

布式拒绝服务攻击事件峰值流量持续突破新高，联网智能设备面临的安全威胁加剧，工业控制系统安全风险在加大，网络攻击“武器库”泄露给网络空间安全造成严重的潜在安全威胁，APT 组织依然活跃等问题，对我国实现建设成为网络强国目标不断提出新的挑战。

国家互联网应急中心（以下简称“CNCERT”）在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 2017 年我国互联网网络安全状况，并预测 2018 年网络安全热点问题。

一、2017 年我国互联网网络安全监测数据分析

（一）恶意程序

1. 计算机恶意程序

据 CNCERT 抽样监测，2017 年我国境内感染计算机恶意程序的主机数量约 1256 万台，同比下降 26.1%，如图 1 所示。位于境外的约 3.2 万个计算机恶意程序控制服务器控制了我国境内约 1101 万台主机，就控制服务器所属国家来看，位于美国、俄罗斯和日本的控制服务器数量分列前三位，分别是 7731 个、1634 个和 1626 个；就所控制我国境内主机数量来看，位于美国、中国台湾和中国香港的控制服务器控制规模分列前三位，分别控制了我国境内约 323 万、42 万和 30 万台主机。

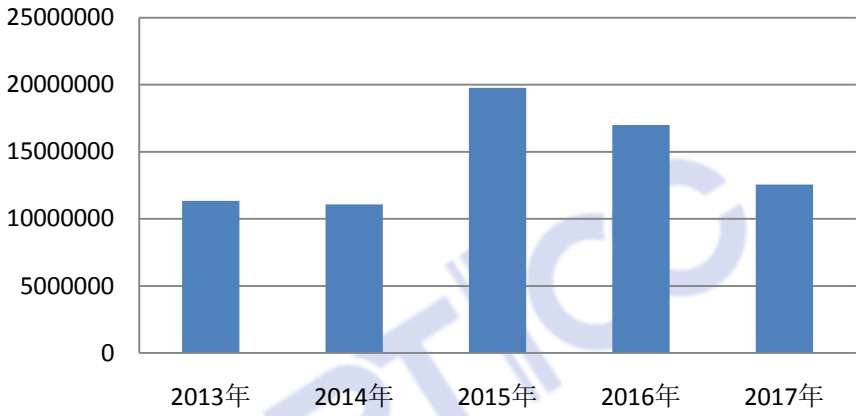

图 1 境内感染计算机恶意程序主机数量变化

根据计算机恶意程序类型分析，我国境内感染远程控制木马、僵尸网络木马和流量劫持木马的主机数量分列前三位，分别达 843 万、239 万和 30 万台主机，如图 2 所示。从我国境内感染计算机恶意程序主机数量按地区分布来看，主要分布在广东省（占我国境内感染数量的 12.5%）、浙江省（占 8.5%）、江苏省（占 7.9%）等网络较为发达的省份，如图 3 所示，但从我国境内感染计算机恶意程序主机数量所占本地区活跃 IP 地址数量比例来看，河南省、青海省和海南省分列前三位。在监测发现的因感染计算机恶意程序而形成的僵尸网络中，规模在 100 台主机以上的僵尸网络数量达 3143 个，规模在 10 万台以上的僵尸网络数量达 32 个，如图 4 所示。为有效控制计算机恶意程序感染主机引发的危害，2017 年，CNCERT 组织基础电信企业、域名服务机构等成功关闭 644 个控制规模较大的僵尸网络。根据第三方的统计报告[③]，位于我国境内的僵尸网络控制端数量保持逐年稳步下降趋势。

[③]相关数据来源于卡巴斯基全球 DDoS 攻击趋势报告（2015.Q1-2017.Q4）。

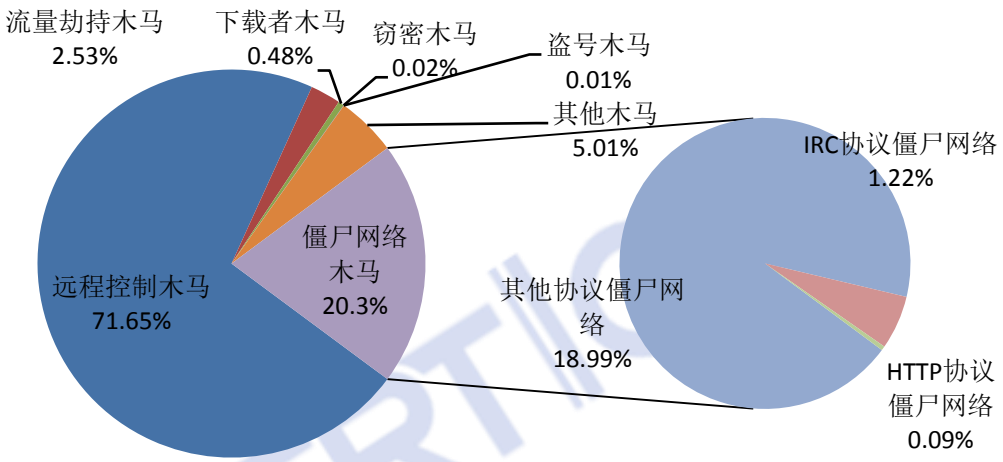

图 2 2017 年计算机恶意程序类型分布

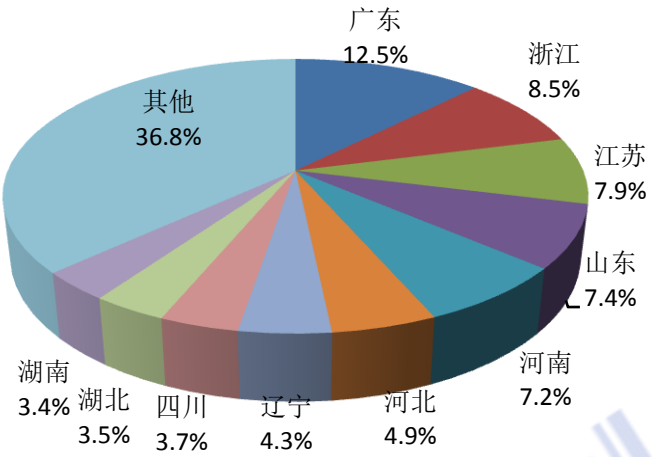

图 3 2017 年境内计算机恶意程序受控主机数量按地区分布

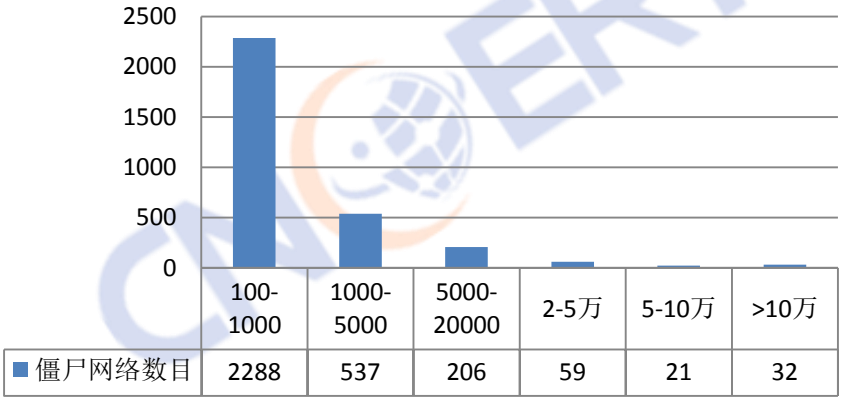

图 4 2017 年僵尸网络的规模分布

2. 移动互联网恶意程序

随着我国 4G 用户平均下载速率的提高、手机流量资费大幅下降，以及银行服务、生活缴费服务、购物支付业务等与网民日常生活紧密相关的服务逐步向移动互联网应用迁移，移动应用程序越来越丰富，给日常的生活带来了极大的便利，但随之而来的移动互联网恶意程序也大量出现，严重危害网民的个人信息安全和财产安全。2017 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 253 万余个，同比增长 23.4%，增长比率为近年来最低，但仍保持高速增长趋势，如图 5 所示。通过对恶意程序的恶意行为统计发现，排名前三的分别为流氓行为类、恶意扣费类和资费消耗类[④]，占比分别为 35.9%、34.3%和 10.4%，如图 6 所示。为有效防范移动互联网恶意程序的危害，严格控制移动互联网恶意程序传播途径，连续 5 年以来，CNCERT 联合应用商店、网盘等服务平台持续加强对移动互联网恶意程序的发现和下架力度，以保障移动互联网健康有序发展。2017 年，CNCERT 累计协调国内 92 家提供移动应用程序下载服务的平台，成功下架 8364 个移动互联网恶意程序，如图 7 所示。

[④] 分类依据为《移动互联网恶意程序描述格式》（标准编号：YD/T 2439-2012）

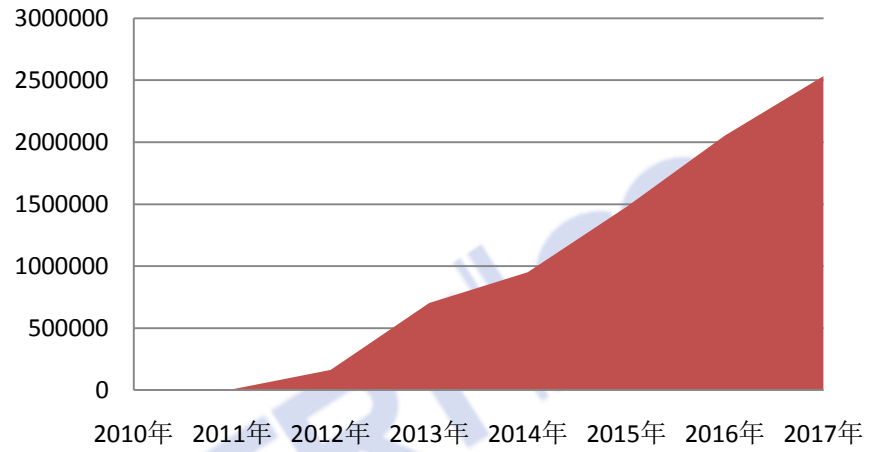

图 5 2010 年至 2017 年移动互联网恶意程序捕获数量走势

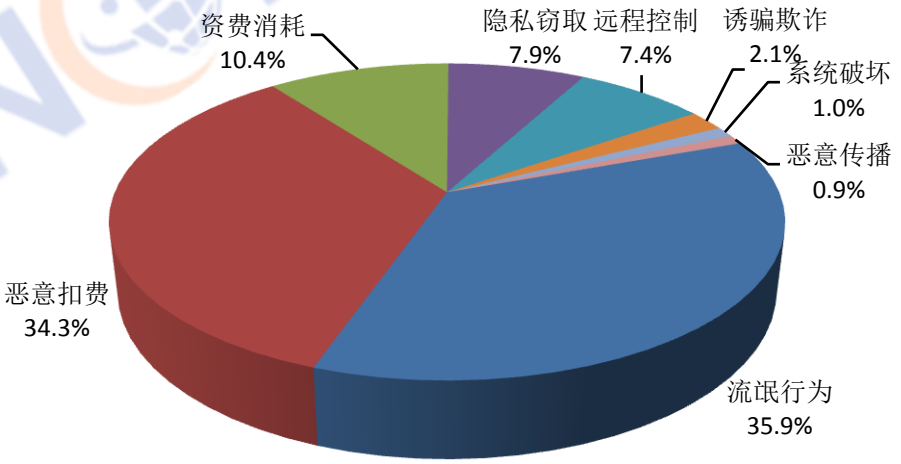

图 6 2017 年移动互联网恶意程序数量按行为属性统计

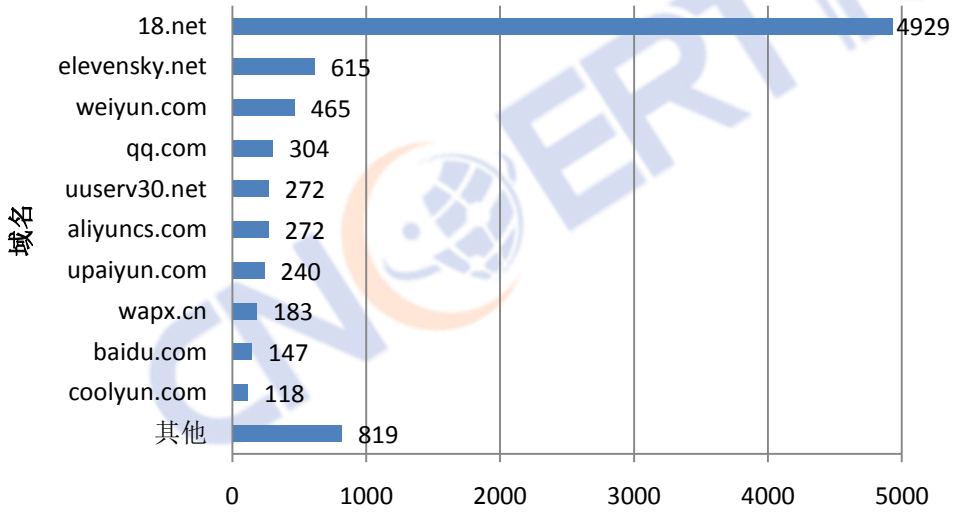

图 7 2017 年各平台成功下架移动互联网恶意程序数量情况

3. 联网智能设备恶意程序

据 CNCERT 监测发现，目前活跃在智能联网设备上的恶意程序家族超过 12 种，主要包括 Ddosf、Dofloo、Gafgyt、MrBlack、Persirai、Sotdas、Tsunami、Triddy、Mirai、Moose、Teaper、Satori 等。这些恶意程序及其变种产生的主要危害包括用户信息和设备数据泄露、硬件设备遭控制和破坏、被用于 DDoS 攻击或其他恶意攻击行为等。CNCERT 抽样监测发现，联网智能设备恶意程序控制服务器 IP 地址约 1.5 万个，位于境外的 IP 地址占比约 81.7%；被控联网智能设备 IP 地址约 293.7 万个；控制联网智能设备形成的僵尸网络有 343 个，其中，控制规模在 1 万台以上的僵尸网络 39 个，5 万台以上的 5 个，如表 1 所示。通过对恶意程序样本分析，发现联网智能设备的恶意程序表现出结构复杂、功能模块分工精细、变种数量多、更新升级快、感染硬件平台广、感染设备种类多等特点，加大了联网智能设备的防护难度。

表 1 2017 年联网智能设备僵尸网络控制规模统计情况

僵尸网络控制规模	僵尸网络个数（按控制端 IP 地址统计）	僵尸网络控制端 IP 地址地理位置分布
5 万以上	5	位于我国境外 3 个，位于我国境内 2 个。
1 万至 5 万	34	均位于我国境外。
5 千至 1 万	38	位于我国境外 37 个，位于我国境内 1 个。
1 千至 5 千	266	均位于我国境外。
10 至 1000	1178	位于我国境外 1153 个，位于我国境内 25 个。

与个人电脑有所不同，家用路由器、家用交换机和网络摄

像头等联网智能设备一般是全天候在线，并且被控后用户不易发现，被黑客控制后作为 DDoS 攻击的“稳定”攻击源。CNCERT 对 Gafgyt 等恶意程序发动的 DDoS 攻击抽样监测发现，DDoS 攻击的控制端 IP 地址和被攻击 IP 地址均主要位于我国境外，但被利用发起DDoS攻击的资源却主要是我国境内大量被入侵控制的联网智能设备。

（二）安全漏洞

1. 安全漏洞收录情况

近年来，国家信息安全漏洞共享平台（CNVD）[5]所收录的安全漏洞数量持续走高。自 2013 年以来，CNVD 收录安全漏洞数量年平均增长率为 21.6%,但 2017 年较 2016 年收录安全漏洞数量增长了 47.4%，达 15955 个，收录安全漏洞数量达到历史新高，如图 8 所示。其中,高危漏洞收录数量高达 5615 个(占 35.2%)，同比增长 35.4%；“零日”漏洞[6]3854 个（占 24.2%），同比增长 75.0%。安全漏洞主要涵盖 Google、Oracle、Microsoft、IBM、Cisco、Apple、WordPress、Adobe、HUAWEI、ImageMagick、Linux 等厂商产品，其中涉及 Google 产品（含操作系统、手机设备以及应用软件等）的漏洞最多，达到 1133 个，占 CNVD 全部收录漏洞的 7.1%，如表 2 所示。按影响对象分类统计，收录漏洞中应用程序漏洞占 59.2%，Web 应用漏洞占 17.6%，操作系统漏洞

[5] 国家信息安全漏洞共享平台（China National Vulnerability Database，简称 CNVD）是由 CNCERT 于 2009 年发起建立的网络安全漏洞信息共享知识库。

[6] “零日”漏洞是指 CNVD 收录该漏洞时还未公布补丁。

占 12.9%，网络设备（如路由器、交换机等）漏洞占 7.7%，安全产品（如防火墙、入侵检测系统等）漏洞占 1.5%，数据库漏洞占 1.1%，如图 9 所示。

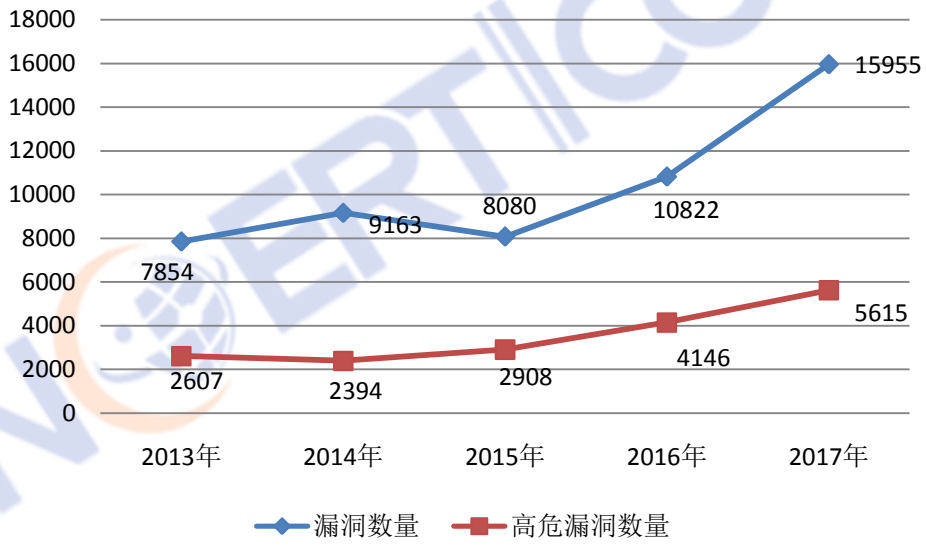

图 8 2013 年至 2017 年 CNVD 收录安全漏洞数量对比

表 2 2017 年 CNVD 收录漏洞涉及厂商情况统计

漏洞涉及厂商	漏洞数量（单位：个）	占全年收录数量百分比	环比
Google	1133	7.1%	38.3%
Oracle	775	4.9%	12.5%
Microsoft	674	4.2%	29.1%
IBM	574	3.6%	14.8%
Cisco	483	3.0%	36.7%
Apple	433	2.7%	-1.4%
WordPress	360	2.3%	54.5%
Adobe	350	2.2%	-37.6%
Huawei	296	1.9%	91.0%
ImageMagick	248	1.6%	/
Linux	228	1.4%	4.6%
其他	10401	65.2%	/

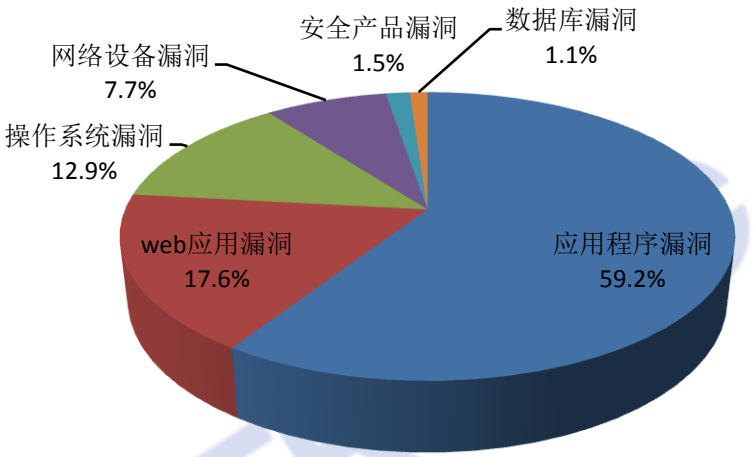

图 9 2017 年 CNVD 收录漏洞按影响对象类型分类统计

2017 年，CNVD 持续推进移动互联网、电信行业、工业控制系统和电子政务 4 类子漏洞库的建设工作，分别新增收录安全漏洞数量 2016 个（占全年收录数量的 12.6%），758 个（占 4.8%），376 个（占 2.4%）和 254 个（占 1.6%），如图 10 所示。其中移动互联网、工业控制系统子漏洞库收录数量较 2016 均有大幅上升，分别增长了 104.7%和 118.6%。

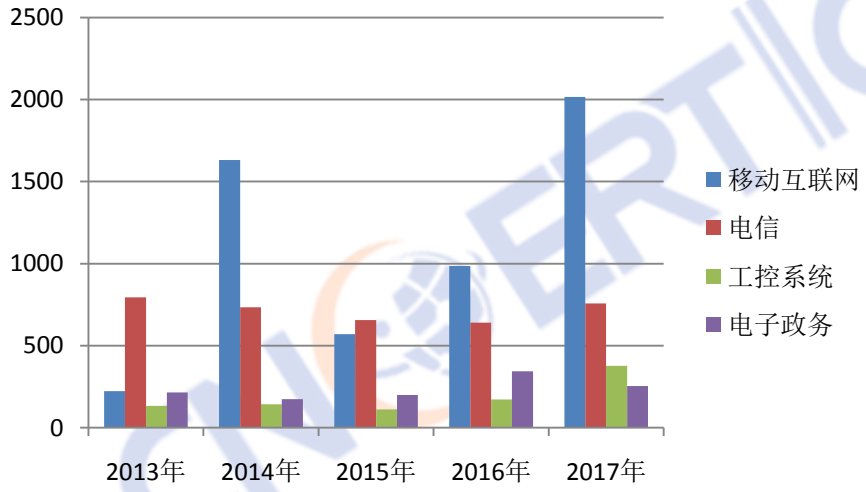

图 10 2013 年至 2017 年 CNVD 子漏洞库收录情况对比

2017 年，CNVD 针对子漏洞库的安全漏洞影响情况进行检测，

全年通报涉及政府机构、关键信息基础设施以及行业安全漏洞事件 26892 起，同比上升 10.9%。

2. 联网智能设备安全漏洞

2017 年，CNVD 收录的安全漏洞中关于联网智能设备安全漏洞有 2440 个，同比增长 118.4%。这些安全漏洞涉及的类型主要包括设备权限绕过、远程代码执行、弱口令等；涉及的设备类型主要包括家用路由器、网络摄像头、会议系统等；涉及的厂商主要是 Google、Cisco、Huawei、D-Link 等。弱口令漏洞是联网智能摄像头的一个威胁高且极易被利用的漏洞类型，CNCERT 持续关注此类漏洞修复情况。2017 年 12 月底，CNCERT 对互联网上暴露的部分品牌智能摄像头弱口令漏洞情况进行监测发现，位于重庆市、四川省、福建省摄像头的弱口令漏洞比例相对较高，如表 3 所示。

表 3 部分品牌的联网智能摄像头 IP 数量分布情况

省（市、区）	部分品牌联网摄像头 IP 数量	部分品牌联网的弱口令摄像头 IP 数量	弱口令摄像头百分比（%）
江苏省	79763	**7024**	8.81
浙江省	74253	**17749**	23.9
山东省	63103	6647	10.53
广东省	49731	**9745**	19.6
河北省	28746	5984	20.82
福建省	27459	6847	**24.94**
辽宁省	27422	3240	11.82
安徽省	26402	4062	15.39
河南省	20184	3227	15.99
云南省	13585	1918	14.12
重庆市	12651	4966	**39.25**
山西省	12595	1966	15.61
四川省	12503	3180	**25.43**

省（市、区）	部分品牌联网摄像头 IP 数量	部分品牌联网的弱口令摄像头 IP 数量	弱口令摄像头百分比（%）
吉林省	12173	1894	15.56
北京市	11271	2270	20.14
上海市	11050	1882	17.03
江西省	9976	1122	11.25
湖南省	9221	1166	12.65
贵州省	8512	230	2.7
黑龙江省	7920	1667	21.05
湖北省	7620	1697	22.27
内蒙古自治区	7115	1099	15.45
陕西省	5988	840	14.03
广西壮族自治区	5435	1184	21.78
新疆维吾尔自治区	5029	601	11.95
天津市	4271	1048	24.54
甘肃省	4059	941	23.18
海南省	3912	808	20.65
宁夏回族自治区	1396	285	20.42
西藏自治区	1356	184	13.57
青海省	977	243	24.87

（三）拒绝服务攻击

据 CNCERT 抽样监测，2017 年我国遭受 DDoS 攻击依然严重，攻击峰值流量持续攀升。为进一步推动 DDoS 攻击的防范打击工作，CNCERT 对全年大流量攻击事件进行深入分析，发现大流量攻击事件的主要攻击方式为 TCP SYN Flood、NTP 反射放大攻击和 SSDP 反射放大攻击。从攻击流量来看，反射放大攻击中的伪造流量来自境外的超过 85%。CNCERT 对 DDoS 攻击资源跟踪分析，发现攻击资源（如控制端、被控端、反射服务器等）发起攻击的次数呈现幂律分布[⑦]的特点，大部分攻击资源发起的攻击次数

[⑦] 幂律分布（Power law distribution），也称长尾分布，这种分布的共性是绝大多数事件的规模很小，而只有少数事件的规模相当大，在双对数坐标下,幂律分布表现为一条斜率为幂指数的负数的直线，这一线性关系是判断给定的实例中随机变量是否满足幂律的依据。统计物理学家习惯于把服从幂律分布的现象称为无标度现象,即系统

只有寥寥数次，而存在少量攻击资源被长期、反复利用发起了大量攻击事件，如图 11-13 所示。其中，发现存在 21 个控制端全年连续 6 个月发起攻击，271 个被控端全年连续 8 个月被利用发起攻击，101 个反射服务器全年连续 8 个月连续被利用发起攻击，这些攻击资源也将作为我们的下一步清理处置工作重点。

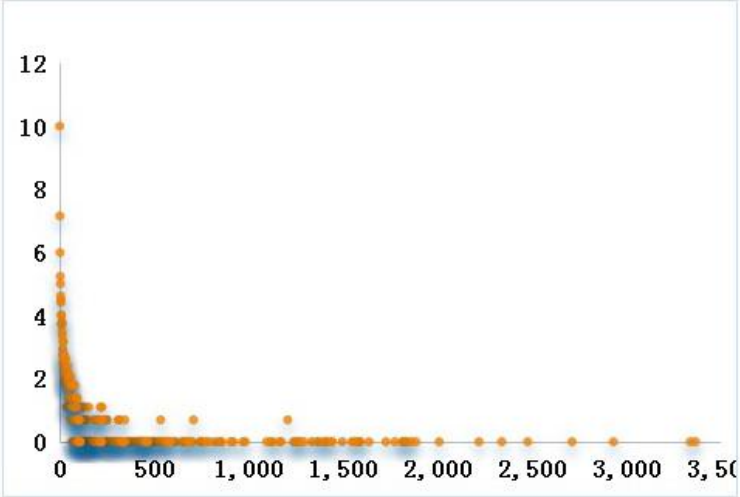

图 11 控制端发起 DDoS 攻击的事件次数呈幂律分布

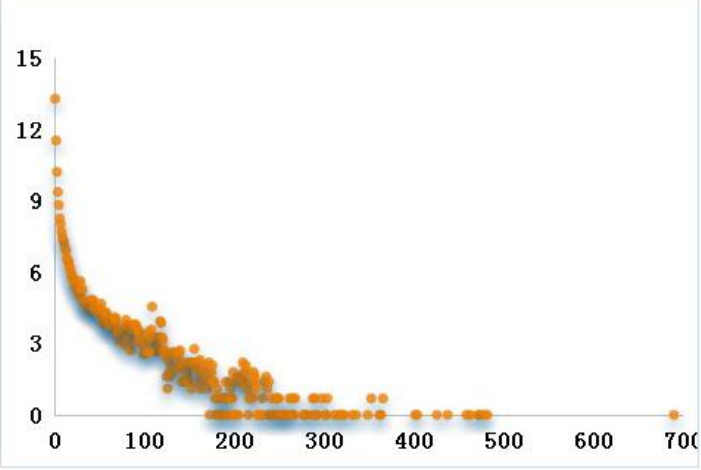

图 12 被控端参与攻击次数呈幂律分布

中个体的尺度相差悬殊。

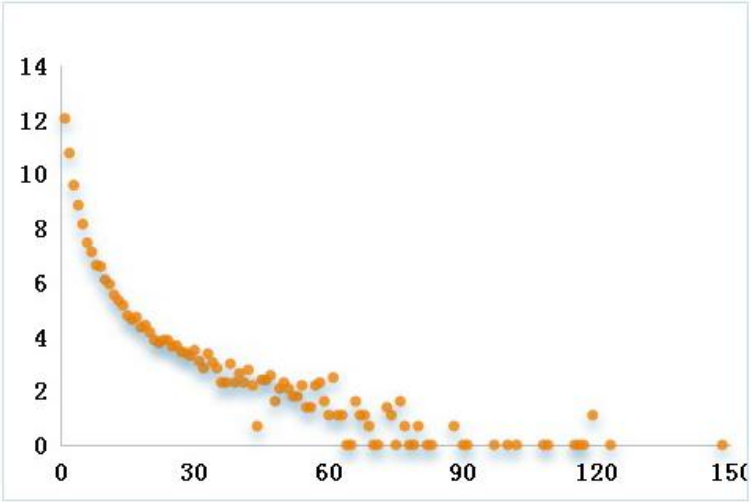

图 13 反射服务器被利用攻击次数呈幂律分布

（四）网站安全

1. 网页仿冒

2017 年，CNCERT 监测发现约 4.9 万个针对我国境内网站的仿冒页面，页面数量较 2016 年的 17.8 万个有大幅下降。为有效防范网页仿冒引起的网民经济损失，CNCERT 重点针对金融行业、电信行业网上营业厅的仿冒页面进行处置，全年共协调处置仿冒页面 2.5 万余个，其中涉及移动互联网的仿冒页面有 7595 个，占全部处置数量的 30.3%。从处置页面的顶级域名来看，“.com”、“.cc”、“.cn” 占比为前三位，其中 “.cn” 的占比同比上升了 7.4%，如图 14 所示。从仿冒类型来看，实名认证和积分兑换仿冒页面最多，分别占处置总数的 30.9%和 20.8%。从承载仿冒页面 IP 地址归属情况来看，同往年一样，大多数位于境外，占比约 88.2%，主要分布在中国香港和美国，其中位于中国香港的 IP 地址超过境外总数的一半，如图 15 所示。

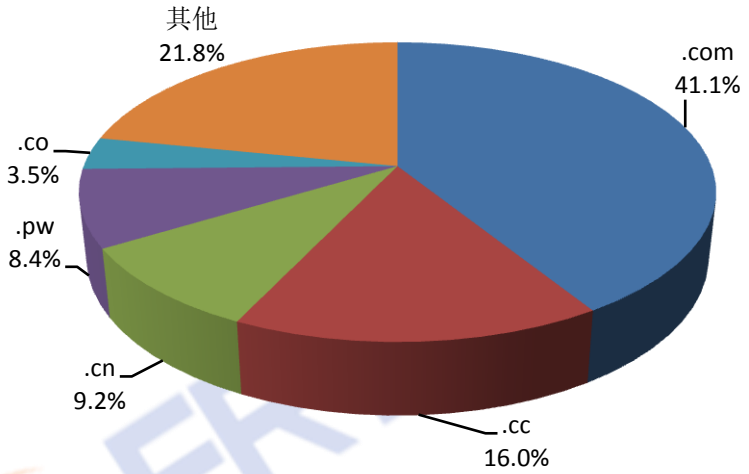

图 14 2017 年仿冒页面所用域名按顶级域分布

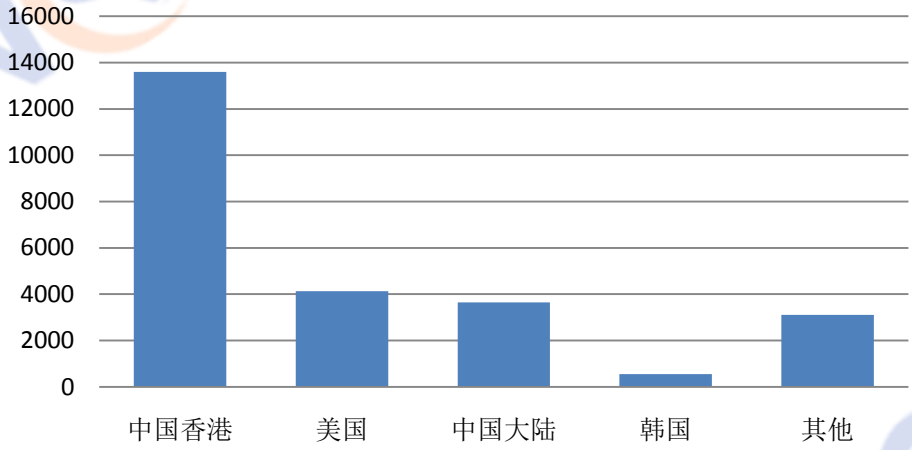

图 15 2017 年承载仿冒页面 IP 地址归属分布

2. 网站后门

CNCERT 监测发现境内外约 2.4 万个 IP 地址对我国境内 2.9 万余个网站植入后门，被植入后门的网站数量较 2016 年的 8.2 万个有大幅下降。约有 2.1 万个（占全部 IP 地址总数的 90.6%）境外 IP 地址对境内约 2.6 万个网站植入后门，其中，位于美国的 IP 地址最多，占境外 IP 地址总数的 10.8%，其次是位于中国香港和俄罗斯的 IP 地址，这与 2016 年的前三位排名一样，如

图 16 所示。从控制我国境内网站总数来看，位于中国香港的 IP 地址控制我国境内网站数量最多，有 4017 个，其次是位于美国和俄罗斯的 IP 地址，分别控制了我国境内 4013 个和 3831 个网站。

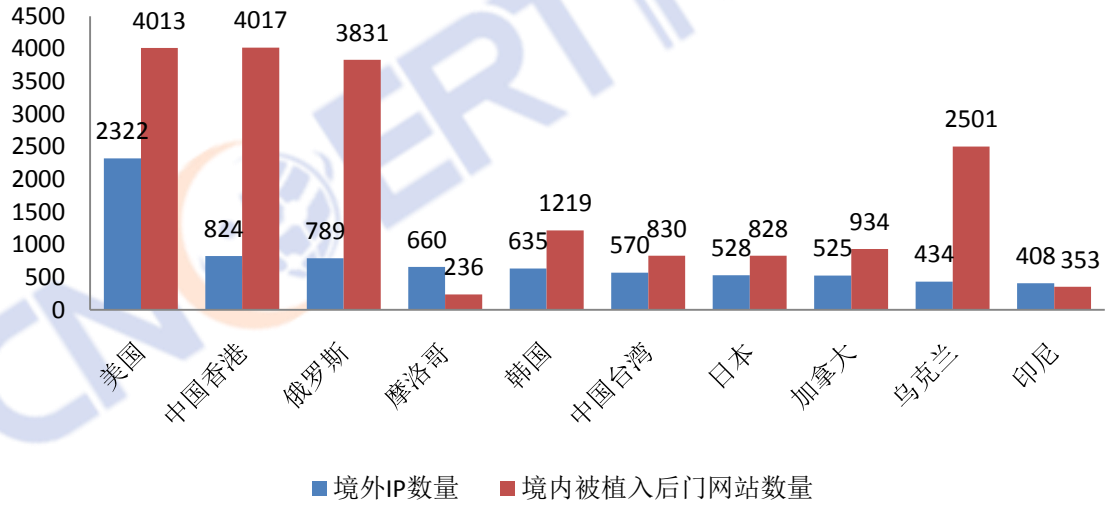

图 16 2017 年境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

3. 网页篡改

2017 年，CNCERT 监测发现我国境内约 2 万个网站被篡改，较 2016 年的约 1.7 万个增长 20.0%，其中被篡改的政府网站有 618 个，较 2016 年的 467 个增长 32.3%，如图 17 所示。从网页被篡改的方式来看，被植入暗链的网站占全部被篡改网站的比例为 68.0%，仍是我国境内网站被篡改的主要方式，但占比较前两年有所下降。从境内被篡改网页的顶级域名分布来看，“.com”、“.net”和“.cn”占比分列前三位，分别占总数的 65.7%、7.6%和 3.1%，如图 18 所示。与 2016 年同期相比，“.com”占比下降了 6.6%，“.net”和“.cn”占比分别上升了 0.3%。

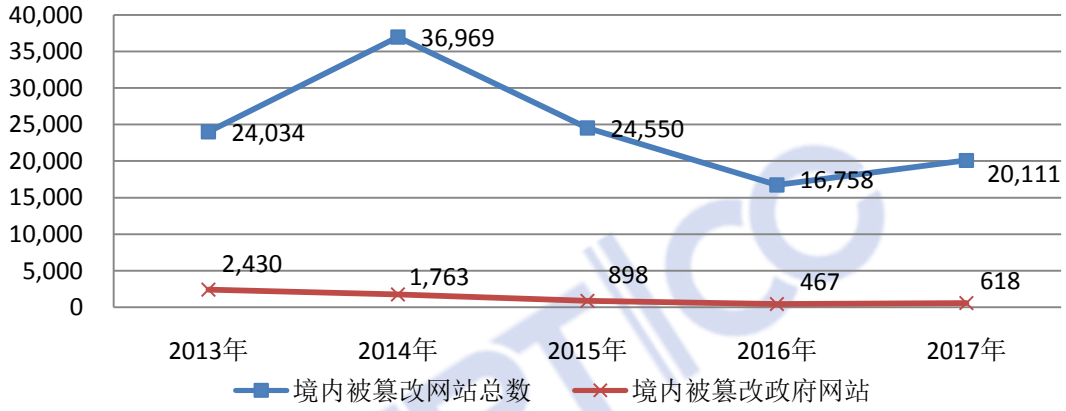

图 17 2013 年至 2017 年我国境内被篡改网站数量情况

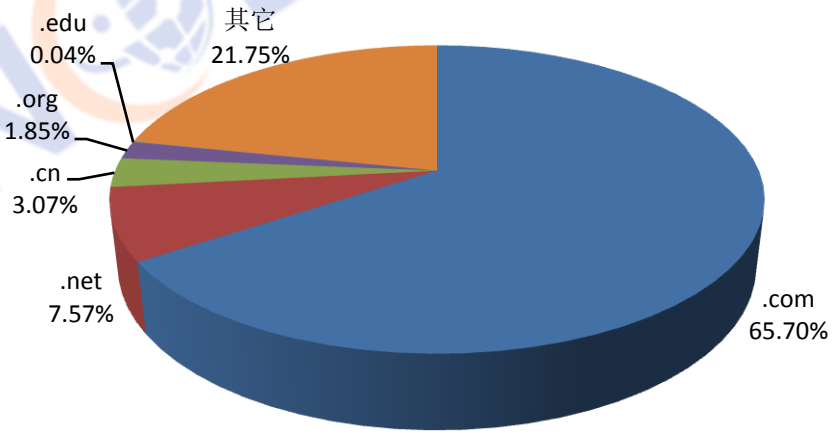

图 18 2017 年境内被篡改网站域名按顶级域分布

（五）工业互联网安全

据 CNCERT 监测，2017 年全年发现超过 245 万起（较上年增长了 178.4%）境外针对我国联网工控系统和设备的恶意嗅探事件，我国境内 4772 个联网工控系统或设备型号、参数等数据信息遭泄露，涉及西门子、摩莎、施耐德等多达 25 家国内外知名厂商的产品和应用，如图 19 所示。同时，2017 年，在 CNVD 工业控制系统子漏洞库中，新增的高危漏洞有 207 个，占该子漏

洞库新增数量的 55.1%，涉及西门子、施耐德、研华科技等厂商的产品和应用，如图 20 所示。在对电力、燃气、供暖、煤炭、水务、智能楼宇六个重点行业的境内联网工控系统或平台开展安全检测过程中，发现存在严重漏洞隐患案例超过 200 例，这些漏洞若被黑客恶意利用，可能造成相关系统生产停摆或大量生产、用户数据泄露，例如通过对全国联网电梯云平台开展网络安全专项检查，发现 30 个平台存在严重安全隐患，影响包括党政军等敏感涉密单位在内的全国 7333 家单位的电梯监控及视频采集系统。

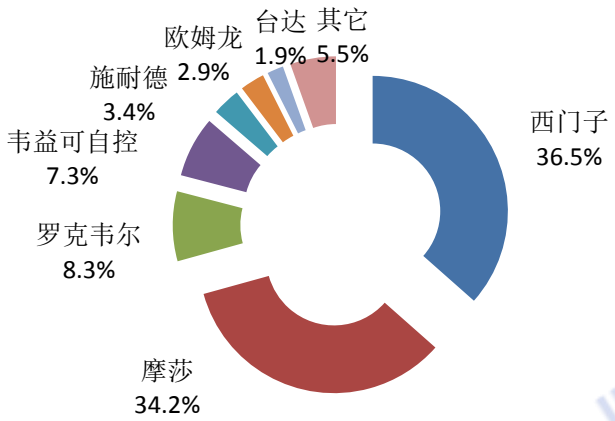

图 19 2017 年发现的联网工控设备厂商分布情况

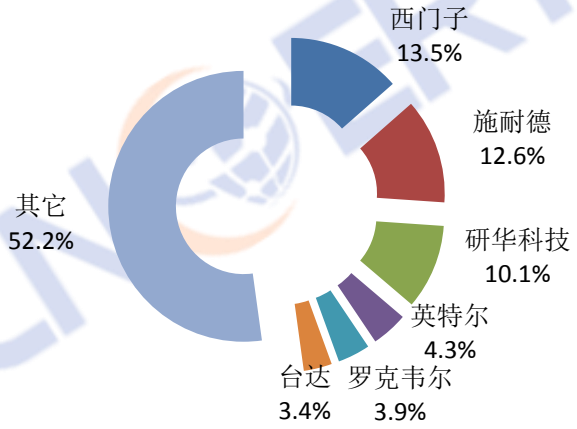

图 20 2017 年工控系统高危漏洞涉及厂商情况

（六）互联网金融安全

近年来，依托大数据、云计算、区块链、移动 APP 等互联网技术和工具，互联网金融实现了多样化的资金融通、支付、交易、信息中介等业务。互联网金融系统承载了大量的用户身份信息、信用信息、资金信息等敏感隐私数据，在存储、传输等过程中一旦发生泄漏、被盗取或被篡改等，都会使各方蒙受巨大损失，甚至影响经济和社会稳定。由于黑客攻击的趋利性，互联网金融成为黑客的重要目标，但大量互联网金融平台网络安全意识淡薄，防护能力不足，进一步加剧了互联网金融面临的网络安全威胁。CNCERT 充分发挥技术优势，着手研究建设了国家互联网金融风险分析技术平台（以下简称“互金技术平台”）。目前，互金技术平台边建设边使用，已经在实际工作中发挥了重要作用，实现了对国家互联网金融安全宏观监测，以及对互联网金融业务的运行异常、网络安全风险的实时监测和预警。2017 年，CNCERT 抽取 1000 余家互联网金融网站进行安全评估检测，发现包括跨站脚本漏洞、SQL 注入漏洞等网站高危漏洞 400 余个，存在严重的用户隐私数据泄露风险，如图 21 所示；对互联网金融相关的移动 APP 抽样检测发现安全漏洞 1000 余个，严重威胁互联网金融的数据安全、传输安全等。

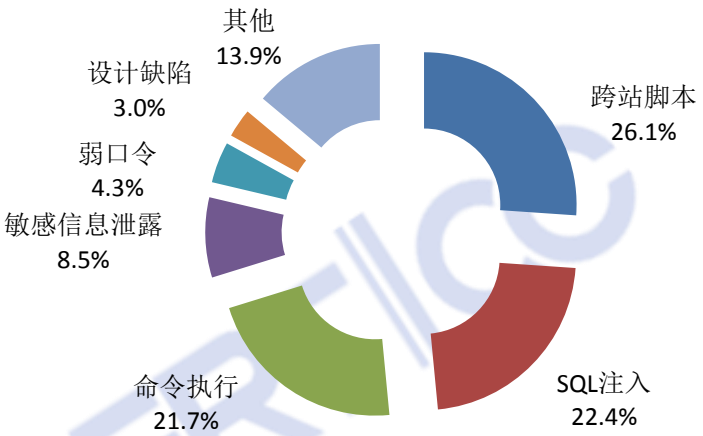

图 21 2017 年互联网金融网站高危漏洞类型分布

二、2017 年我国互联网网络安全状况

（一）我国网络空间法治进程迈入新时代

2017 年 6 月 1 日，《中华人民共和国网络安全法》（以下简称“网络安全法”）正式实施，我国网络安全管理的综合法律体系建设正式启航。在推动网络安全法落地方面，配套法律法规和规范性文件相继出台，包括《国家网络安全应急预案》、《网络产品和服务安全审查办法（试行）》、《网络关键设备和网络安全专用产品目录（第一批）》、《公共互联网网络安全威胁监测与处置办法》、《公共互联网网络安全突发事件应急预案》、《个人信息和重要数据出境安全评估办法（征求意见稿）》、《关键信息基础设施安全保护条例（征求意见稿）》等，我国网络空间法治体系建设加速开展。在标准制定方面，全国信息安全标准化技术委员会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国家标准的研究。在开展网络安全宣传教育方面，2017 年国家网络安全宣传周期间，以校园、电信、法制等为主题设置宣传日，针对社会公众关注的网络热点问题，举办网络安全体验展等系列主题宣传活动，营造网络安全人人有责、人人参与的良好氛围。

（二）网络反诈工作推进 仿冒页面数量剧减并向境外转移

随着我国互联网技术的快速发展和普及，通过互联网实施

经济诈骗的事件多有发生，诈骗方式也多种多样。其中，仿冒页面作为网络诈骗主要方式之一，给我国网民经济安全带来严重威胁。CNCERT 持续开展仿冒页面处置工作，在 2017 年协调处置的仿冒页面中，域名在境外注册的比例为 43.9%，同比上升了 14.2%，承载仿冒页面的 IP 地址 88.2%位于境外，同比上升了 7.8%，仿冒我国境内网站的仿冒页面域名注册和 IP 地址均表现出向境外迁移趋势。对所处置的仿冒页面所属域名注册商分析发现，所属注册商占比最高的为 GoDaddy，而在 2016 年，GoDaddy 未进入前十名。为有效加强仿冒页面的处置工作，CNCERT 通过建立的广泛国际合作途径，积极向国外 CERT 组织、域名注册商等通报仿冒页面信息，协调国际合作伙伴尽快对仿冒我国境内网站的页面进行处置。2017 年，CNCERT 向国际合作伙伴投诉仿冒页面事件达 1.7 万余次，其中向位于中国香港、美国、印度的机构投诉次数最多，分别达 7684 次、6719 次、1180 次。

（三）“网络武器库”泄露后风险威胁凸显

近年来，黑客组织的工具库或文件泄露事件引发大家普遍关注。2015 年，间谍软件公司“Hacking Team”被攻击，多达 400GB 的数据外泄。2016 年 8 月以来，黑客组织“影子经纪人”陆续公布“方程式”组织[®]经常使用的工具包，包含各种防火墙的漏洞利用代码、植入固件、代码说明和部分受攻击目标的 IP

[®]“方程式”组织是由最早发现的卡巴斯基实验室命名，研究表明该组织为美国家安全局（NSA）开发网络攻击工具。

和域名列表等。2017 年 3 月，维基解密声称美国中情局（CIA）用于网络攻击的大量病毒木马、远程控制、0day 漏洞以及相关文档已被泄露，并将其获得的一部分文档分七批次（并称“Vault7”）在其官方网站公开发布。这些资料在被公开之初，因相关的防范措施还未及时提出，相关的网络安全防护技术还未落实，若被滥用可能引发重大网络安全事件，给网络空间安全带来严重威胁。2017 年 4 月 14 日晚，“影子经纪人”在互联网上公布了“方程式”使用的包含针对微软操作系统以及其他办公、邮件软件的多个高危漏洞攻击工具包，这些工具集成化程度高、部分攻击利用方式较为高效。在时隔不到一个月，5 月 12 日 WannaCry 蠕虫病毒事件爆发，并随后迅速出现了多款变种。该系列病毒就是利用了“影子经纪人”公开的微软操作系统“永恒之蓝”漏洞进行快速传播，给全球网络空间安全造成了严重影响，WannaCry 蠕虫病毒事件是“网络武器库”遭泄露引发的重大网络安全事件典型代表。

（四）敲诈勒索和“挖矿”等牟利恶意攻击事件数量大幅增长

2017 年出现的 Petya、NotPetya、BadRabbit 等危害严重的恶意程序再度掀起敲诈勒索软件的热度。2017 年，CNCERT 捕获新增勒索软件近 4 万个，呈现快速增长趋势。到 2017 年下半年，随着比特币、以太币、门罗币等数字货币的价值暴涨，导致针

对数字货币交易平台的网络攻击越发频繁，同时引发了更多利用勒索软件向用户勒索数字货币的网络攻击事件和用于“挖矿”的恶意程序数量大幅上升，并推动了区块链技术的大热。“挖矿”恶意程序大量占用和消耗计算机的 CPU 等资源，会使得计算机性能变低，运行速度变慢，其非破坏性和隐蔽性使得用户难以发现。我们也注意到，勒索或“挖矿”恶意程序综合利用多种网络攻击手段，实现短期内大规模地感染用户计算机，如 Petya 利用了微软 Windows SMB 服务漏洞大规模传播，BadRabbit 恶意代码伪装成 Adobe Flash 升级更新弹窗诱导用户主动点击下载并运行。

（五）应用软件供应链安全问题触发连锁反应

自 2015 年以来，应用软件供应链被污染事件多有发生，9 月爆出苹果开发工具 Xcode 被植入 XcodeGhost 恶意代码，导致使用该工具开发的苹果 APP 被植入恶意代码。同年 10 月，网上披露了“WormHole”漏洞，该漏洞存在于国内某公司开发的一款公共开发套件中，影响集成此套件的该公司系列 APP 及其它 20 余款 APP。进入 2017 年，应用软件供应链安全问题集中爆发。8 月，NetSarang 公司旗下的 Xshell、Xmanager 等多款产品被曝存在后门问题。Xshell 是一款应用广泛的终端模拟软件，被用于服务器运维和管理，此次的后门问题可导致敏感信息被泄露。据 CNCERT 监测结果，我国网络空间运行 Xshell 等相关软

件的 IP 地址有 3.1 万余个。2017 年还曝出的惠普笔记本音频驱动内置键盘记录后门、CCleaner 后门等，均对我国网络空间安全带来巨大隐患，对我国互联网的稳定运行和信息数据的安全构成严重威胁。

三、2018 年值得关注的热点

（一）个人信息和重要数据保护立法呼声日益高涨

根据公开数据统计，2017 年数据泄露事件数量较近几年来有增无减，且泄露的数据总量创历史新高。2017 年 3 月，公安部公布破获一起盗卖我国公民信息的特大案件，犯罪团伙涉嫌入侵社交、游戏、视频直播、医疗等各类公司的服务器，非法获取用户账号、密码、身份证、电话号码、物流地址等重要信息 50 亿条。随着信息数据经济价值上升，促使攻击者利用多种攻击手段从多种渠道获取更多敏感数据，我们相信窃取用户个人信息和数据的网络攻击活动并不会消退。在当前网民越来越注重个人信息安全，并意识到信息泄露可能带来的个人人身财产安全问题，希望政府加强监管、企业落实数据保护的呼声越来越高。

（二）安全漏洞信息保护备受关注

根据 CNVD 收录漏洞的情况，近三年来新增通用软硬件漏洞的数量年均增长超过 20%，漏洞收录数量呈现快速增长趋势。信息系统存在安全漏洞是诱发网络安全事件的重要因素，而 2017 年，CNVD“零日”漏洞收录数量同比增长 75.0%，这些漏洞给网络空间安全带来严重安全隐患，加强安全漏洞的保护工作显得尤为重要。根据《网络安全法》第二十六条规定，向社会发布

系统漏洞应当遵守国家有关规定。近年来，多起“网络攻击武器库”泄露事件进一步扩大了安全漏洞可能造成的严重危害，落实法律要求，进一步细化我国安全漏洞信息保护管理工作迫在眉睫。

（三）物联网设备面临的网络安全威胁加剧

2018 年，我们将继续看到一些物联网设备被利用发动攻击。2017 年 CNVD 收录的物联网设备安全漏洞数量较上年增长近 1.2 倍，每日活跃的受控物联网设备 IP 地址达 2.7 万个。我国在 2017 年下半年密集出台了推进 IPv6、5G、工业互联网等多项前沿科技发展的政策，并要求 2018 年开展商用试点工作，这将助推物联网更快的普及和物联网设备数量快速的增长。但由于设备制造商安全能力不足和行业监管还未完善，2018 年物联网设备的安全威胁将加剧，对用户的个人隐私、资金财产乃至人身安全造成极大危害，亟需可实施的防护解决方案。

（四）数字货币将引发更多更复杂的网络攻击

数字货币市场的“繁荣”，直接带来了 2017 年勒索软件、挖矿木马的增长势头，且将会延续到 2018 年。为了寻求更多的“挖矿工具”，提高“挖矿”能力，网络攻击者将会综合利用多种网络攻击手段，包括安全漏洞、恶意邮件、网页挂马、应用仿冒等，对目标实施网络攻击，且攻击方式会越来越复杂和难

以发现。

（五）人工智能运用在网络安全领域热度持续上升

自 2016 年人工智能、机器学习概念兴起以来，人工智能应用在网络安全领域的研究已经取得一定成绩。多个科技公司开始研究打造由人工智能技术驱动的安全体系，建立能够跨网络和平台部署的人工智能安全系统，以监控、发现和防止黑客入侵。但同时，黑客也正在利用人工智能和机器学习为发起攻击提供技术支持，一方面是对人工智能应用发起攻击，另一方面与防御方竞赛，更快地发现并利用新漏洞。随着网络空间网络安全环境的日益复杂，攻防双方日益激烈的较量中，人工智能与机器学习的关注度将持续上升。