2019 年上半年我国互联网网络安全态势

国家计算机网络应急技术处理协调中心

2019 年 8 月

目　录

为维护我国网络空间的安全，保障互联网健康有序的发展，2019 年上半年，我国持续推进网络安全法律法规体系建设，完善网络安全管理体制机制，不断加强互联网网络安全监测和治理，构建互联网发展安全基础，构筑网民安全上网环境。2019 年上半年，我国基础网络运行总体平稳，未发生较大规模以上网络安全事件。但数据泄露事件及风险、有组织的分布式拒绝服务攻击干扰我国重要网站正常运行、鱼叉钓鱼邮件攻击事件频发，多个高危漏洞被曝出，我国网络空间仍面临诸多风险与挑战。

一、2019 年上半年我国互联网网络安全监测数据分析

国家互联网应急中心（以下简称“CNCERT”）从恶意程序、漏洞隐患、移动互联网安全、网站安全以及云平台安全、工业系统安全、互联网金融安全等方面，对我国互联网网络安全环境开展宏观监测。数据显示，与 2018 年上半年数据比较，2019 年上半年我国境内通用型“零日”漏洞[①]收录数量，涉及关键信息基础设施的事件型漏洞通报数量，遭篡改、植入后门、仿冒网站数量等有所上升，其他各类监测数据有所降低或基本持平。

（一）恶意程序

1. 计算机恶意程序捕获情况

2019 年上半年，CNCERT 新增捕获计算机恶意程序样本

[①] “零日”漏洞是指 CNVD 收录该漏洞时还未公布补丁。

数量约 3,200 万个，与 2018 年上半年基本持平，计算机恶意程序传播次数日均达约 998 万次。按照计算机恶意程序传播来源统计，位于境外的 IP 地址主要是来自美国、日本和菲律宾等国家和地区，2019 年上半年计算机恶意代码传播源位于境外分布情况如图 1 所示。位于境内的 IP 地址主要是位于广东省、北京市和浙江省等。按照受恶意程序攻击的 IP 统计，我国境内受计算机恶意程序攻击的 IP 地址约 3,762 万个，约占我国活跃 IP 地址总数的 12.4%，这些受攻击的 IP 地址主要集中在江苏省、广东省、浙江省等地区，2019 年上半年我国境内受计算机恶意程序攻击的 IP 分布情况如图 2 所示。

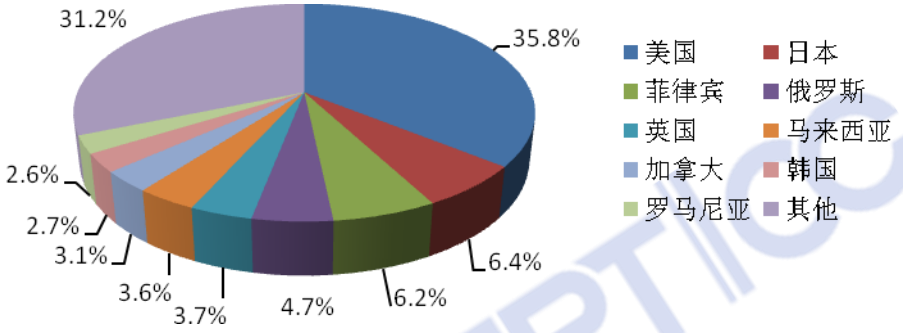

图 1 2019 年上半年计算机恶意代码传播源位于境外分布情况

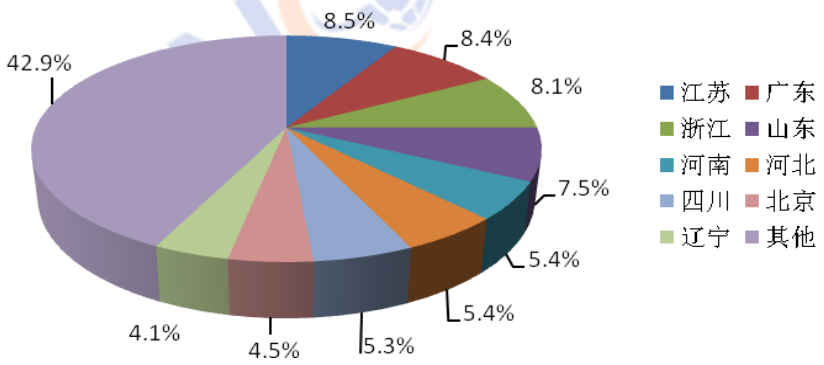

图 2 2019 年上半年我国受计算机恶意代码攻击的 IP 分布情况

2. 计算机恶意程序用户感染情况

据 CNCERT 抽样监测，2019 年上半年，我国境内感染计算机恶意程序的主机数量约 240 万台，相较 2018 年上半年同比下降 9.7%。位于境外的约 3.9 万个计算机恶意程序控制服务器控制了我国境内约 210 万台主机，就控制服务器所属国家来看，位于美国、日本和拉脱维亚的控制服务器数量分列前三位，分别是约 9,494 个、5,535 个和 2,350 个；就所控制我国境内主机数量来看，位于美国、法国和英国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 150 万、22 万和 16 万台主机。

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 13.3%）、河南省（占 11.0%）、山东省（占 7.0%）等省份，但从我国境内各地区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、云南省和河北省分列前三位，如图 3 所示。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 1,842 个，规模在 10 万台以上的僵尸网络数量达 21 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，2019 年上半年，CNCERT 组织基础电信企业、域名服务机构等成功关闭 714 个控制规模较大的僵尸网络。

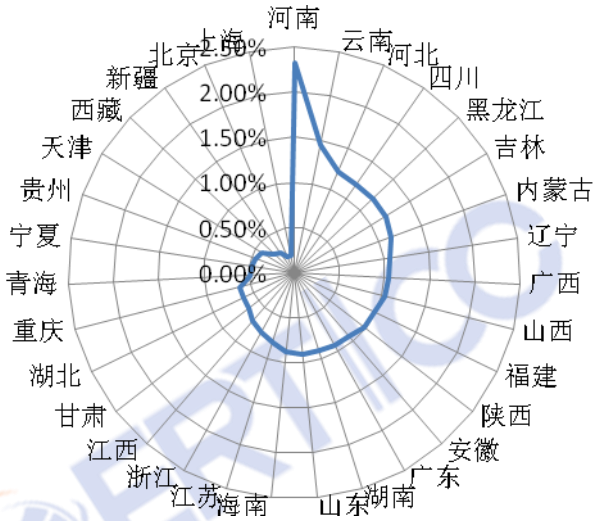

图 3 我国各地区感染计算机恶意程序主机数量占本地区活跃 IP 地址数量比例

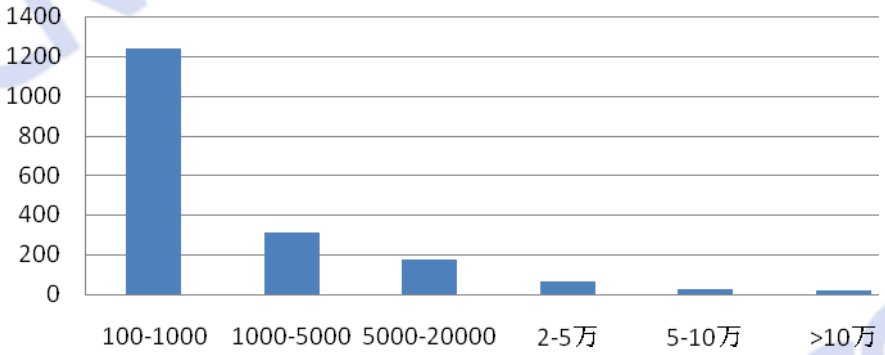

图 4 2019 年上半年僵尸网络的规模分布

3. 移动互联网恶意程序

2019 年上半年，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 103 万余个，同比减少 27.2%。通过对恶意程序的恶意行为统计发现，排名前三的分别为资费消耗类、流氓行为类和恶意扣费类，占比分别为 35.7%、27.1%和 15.7%。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 7 年以来，CNCERT 联合应用商店、云平台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。2019 年上半年，CNCERT 累计协调国内 177 家提供移动应用程序下载服务的平台，下架 1,190 个移动互联网恶意程序。

近年来，新型网络诈骗手法层出不穷，随着移动互联网和普惠金融的大力发展，出现了大量以移动端为入口骗取用户个人隐私信息和账户资金的网络诈骗活动。据 CNCERT 抽样监测，2019 年上半年以来，我国以移动互联网为载体的虚假贷款 APP 或网站达 1.5 万个，在此类虚假贷款 APP 或网站上提交姓名、身份证照片、个人资产证明、银行账户、地址等个人隐私信息的用户数量超过 90 万。大量受害用户在诈骗平台支付了上万元的所谓“担保费”、“手续费”费用，经济利益受到实质损害。

4. 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主要包括 Mirai、Gafgyt、MrBlack、Tsunami、Reaper、Ddostf、Satori、TheMoon、StolenBots、VPNFilter、Cayosin 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、攻击路由器等网络设备窃取用户上网数据等。CNCERT 抽样监测发现，2019 年上半年，联网智能设备恶意程序控制服务器 IP 地址约 1.9 万个，同比

上升 11.2%；被控联网智能设备 IP 地址约 242 万个，其中位于我国境内的 IP 地址近 90 万个（占比 37.1%），同比下降 12.9%；通过控制联网智能设备发起 DDoS 攻击次数日均约 2,118 起。

（二）安全漏洞

1. 安全漏洞收录情况

2019 年上半年，国家信息安全漏洞共享平台（以下简称“CNVD”）收录通用型安全漏洞 5,859 个，同比减少 24.4%，其中高危漏洞收录数量为 2,055 个（占 35.1%），同比减少 21.2%，“零日”漏洞收录数量为 2,536 个（占 43.3%），同比增长 34.0%。安全漏洞主要涵盖 Google、Microsoft、Adobe、Cisco、IBM 等厂商产品。按影响对象分类统计，收录漏洞中应用程序漏洞占 56.2%，Web 应用漏洞占 24.9%，操作系统漏洞占 8.3%，网络设备（如路由器、交换机等）漏洞占 7.6%，数据库漏洞占 1.8%，安全产品（如防火墙、入侵检测系统等）漏洞占 1.2%，如图 5 所示。

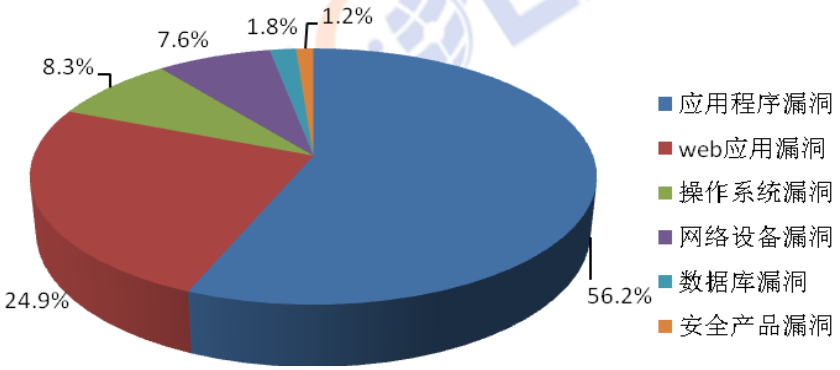

图 5 2019 年上半年 CNVD 收录漏洞按影响对象类型分类统计

2019 年上半年，CNVD 继续推进移动互联网、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 384 个（占收录数量的 6.6%）、323 个（占 5.5%）、158 个（占 2.7%）和 87 个（占 1.5%）。

2. 联网智能设备安全漏洞

2019 年上半年，CNVD 收录的安全漏洞中关于联网智能设备安全漏洞有 1,223 个，与 2018 年上半年基本持平。这些安全漏洞涉及的类型主要包括设备信息泄露、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、网络摄像头等。

（三）拒绝服务攻击

CNCERT 抽样监测发现，2019 年上半年我国境内峰值超过 10Gbps 的大流量分布式拒绝服务攻击（以下简称“DDoS 攻击”）事件数量平均每月约 4,300 起，同比增长 18%，并且仍然是超过 60%的 DDoS 攻击事件为僵尸网络控制发起。在 DDoS 攻击资源分析方面，2019 年上半年，CNCERT 发现用于发起 DDoS 攻击的 C&C 控制服务器[②]数量共 1,612 个，其中位于我国境内的有 144 个，约占总量的 8.9%，同比减少 13%，位于境外的控制端数量同比增长超过一倍；总肉鸡[③]数量约 64 万个，同比下降 10%；反射攻击服务器约 617 万个，

[②] C&C 控制服务器：全称为 Command and Control Server，即“命令及控制服务器”，目标机器可以接收来自服务器的命令，从而达到服务器控制目标机器的目的。

[③] 肉鸡：接收来自 C&C 控制服务器指令，对外发出大量流量的被控联网设备。

同比下降 33%；受攻击目标 IP 地址数量约 5.7 万余个，这些攻击目标主要分布在色情、博彩等互联网地下黑产方面以及文化体育和娱乐领域。

（四）网站安全

1. 网页仿冒

2019 年上半年，CNCERT 自主监测发现约 4.6 万个针对我国境内网站的仿冒页面。为有效防范网页仿冒引发的危害，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，共协调处置仿冒页面 1.2 万余个，同比减少 35.2%。对这些已协调处置的仿冒页面分析来看，承载仿冒页面 IP 地址归属情况与近几年来的情况一样，主要分布在美国和中国香港，如图 6 所示。

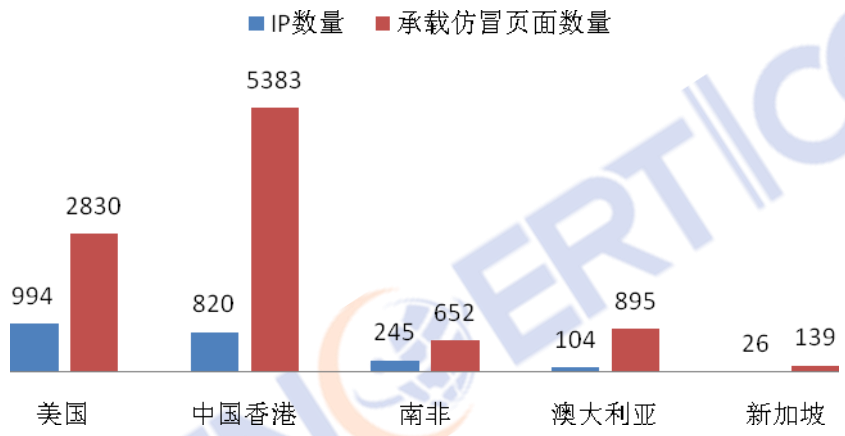

图 6 2019 年上半年承载仿冒页面 IP 地址和仿冒页面数量分布

2. 网站后门

2019 年上半年，CNCERT 监测发现境内外约 1.4 万个 IP 地址对我国境内约 2.6 万个网站植入后门，同比增长约 1.2

倍。其中，约有 1.3 万个（占全部 IP 地址总数的 91.2%）境外 IP 地址对境内约 2.3 万个网站植入后门，位于美国的 IP 地址最多，其次是位于中国香港和新加坡的 IP 地址，如图 7 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 6,984 个，其次是位于美国和菲律宾的 IP 地址，分别控制了我国境内 4,816 个和 2,509 个网站。

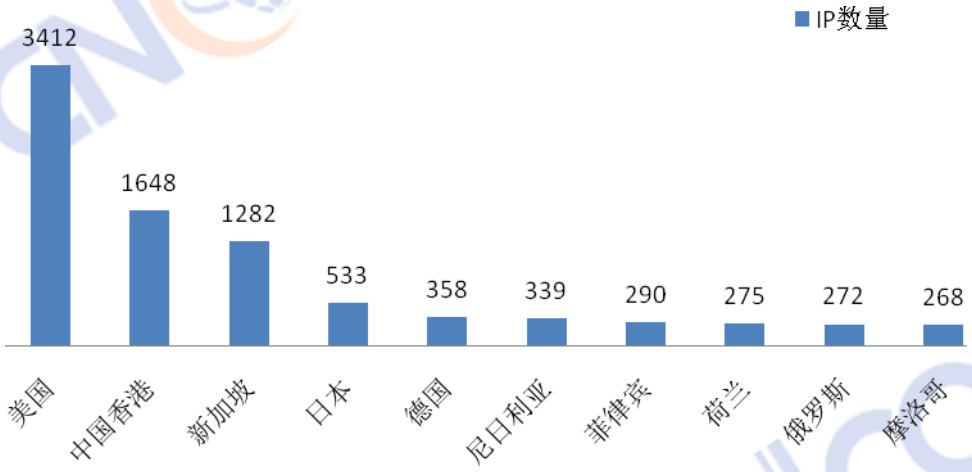

图 7 2019 年上半年向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

3. 网页篡改

2019 年上半年，CNCERT 监测发现并协调处置我国境内遭篡改的网站有近 4 万个，其中被篡改的政府网站有 222 个。从境内被篡改网页的顶级域名分布来看，“.com”、“.net”和“.org”占比分列前三位，如图 8 所示。

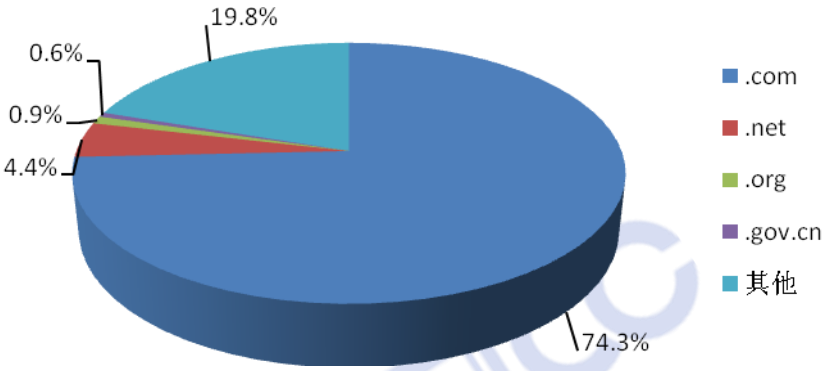

图 8 2019 年上半年我国境内被篡改网站数量按类型分布

（五）云平台安全

根据 CNCERT 监测数据，2019 年上半年，发生在我国云平台上的网络安全事件或威胁情况相比 2018 年进一步加剧。首先，发生在我国主流云平台上的各类网络安全事件数量占比仍然较高，其中云平台上遭受 DDoS 攻击次数占境内目标被攻击次数的 69.6%、被植入后门链接数量占境内全部被植入后门链接数量的 63.1%、被篡改网页数量占境内被篡改网页数量的 62.5%。其次，攻击者经常利用我国云平台发起网络攻击，其中利用云平台发起对我国境内目标的 DDoS 攻击次数占监测发现的 DDoS 攻击总次数的 78.8%、发起对境内目标 DDoS 攻击的 IP 地址中来自我国境内云平台的 IP 地址占 72.4%、承载的恶意程序种类数量占境内互联网上承载的恶意程序种类数量的 71.2%、木马和僵尸网络恶意程序控制端 IP 地址数量占境内全部恶意程序控制端 IP 地址数量的 84.6%。另外，自 2019 年以来，CNCERT 在持续开展的

MongoDB、Elasticsearch 等数据库数据泄露风险应急处置过程中，发现存在隐患的数据库搭建在云服务商平台上的数量占比超过 40%。云服务商和云用户应加大对网络安全的重视和投入，分工协作提升网络安全防范能力。云服务商应提供基础性的网络安全防护措施并保障云平台安全运行，全面提高云平台的安全性和可控性，全面加强网络安全事件监测和处置能力。云用户对部署在云平台上的系统承担主体责任，需全面落实系统的网络安全防护要求。

（六）工业互联网安全

1. 工业网络产品安全检测情况

电力安全是关键信息基础设施保护的重要内容之一，为调查我国电力二次设备的安全现状，2019 年上半年 CNCERT 继续对国内主流电力厂商的产品进行安全摸底测试，电力设备供应商在电网企业的引导下，已有一定安全意识，但设备整体网络安全水平仍有待提高。截至目前，在涉及 28 个厂商、70 余个型号的六大类产品（测控装置、保护装置、智能远动机、站控软件、PMU、网络安全态势感知采集装置，）中均发现了中、高危漏洞，可能产生的风险包括拒绝服务攻击、远程命令执行、信息泄露等。其中 SISCO MMS 协议[④]开发套件漏洞，几乎影响到每一款支持 MMS 协议的电力装置。

[④]制造报文规范（MMS）协议是 ISO 9506 标准所定义的一套用于工业控制系统的通信协议，目的是为了规范工业领域具有通信能力的智能传感器、智能电子设备、智能控制设备的通信行为，使系统集成变得简单、方便。

2. 联网工业设备和工业云平台暴露情况

2019 年上半年，CNCERT 进一步加强了针对联网工业设备和工业云平台的网络安全威胁发现能力，累计监测发现我国境内暴露的联网工业设备数量共计 6,814 个，包括可编程逻辑控制器、数据采集监控服务器、串口服务器等，如图 9 所示，涉及西门子、韦益可自控、罗克韦尔等 37 家国内外知名厂商的 50 种设备类型。其中，存在高危漏洞隐患的设备占比约 34%，这些设备的厂商、型号、版本、参数等信息长期遭恶意嗅探，仅在 2019 年上半年嗅探事件就高达 5,151 万起。另外，CNCERT 发现境内具有一定用户规模的大型工业云平台 40 余家，业务涉及能源、金融、物流、智能制造、智慧城市、医疗健康等方面，并监测到根云、航天云网、COSMOPlat、OneNET、OceanConnect 等大型工业云平台持续遭受漏洞利用、拒绝服务、暴力破解等网络攻击，工业云平台已经成为网络攻击的重点目标。

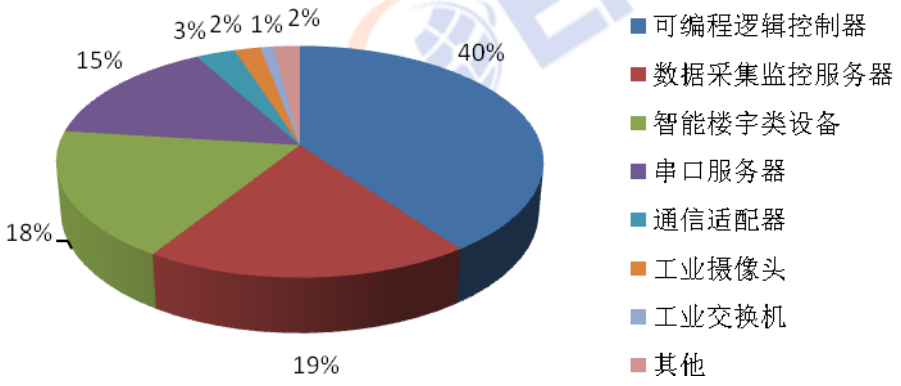

图 9 2019 年上半年发现的联网工业设备类型分布情况

3. 重点行业安全情况

涉及国计民生的重点行业监控管理系统因存在网络配置疏漏等问题，可能会直接暴露在互联网上，一旦遭受网络攻击，影响巨大。为评估重要行业联网系统的网络安全风险情况，2019 年上半年 CNCERT 对水电和医疗健康两个行业的联网监控或管理系统开展了网络安全监测与分析，发现水电行业暴露相关监控管理系统 139 个，涉及生产管理和生产监控 2 大类；医疗健康行业暴露相关数据管理系统 709 个，涉及医学信息和基因检测 2 大类，如图 10 所示。同时，CNCERT 监测发现，在以上水电和健康医疗行业暴露的系统中，存在高危漏洞隐患的系统占比分别为 25%和 72%，且部分暴露的监控或管理系统存在遭境外恶意嗅探、网络攻击情况。

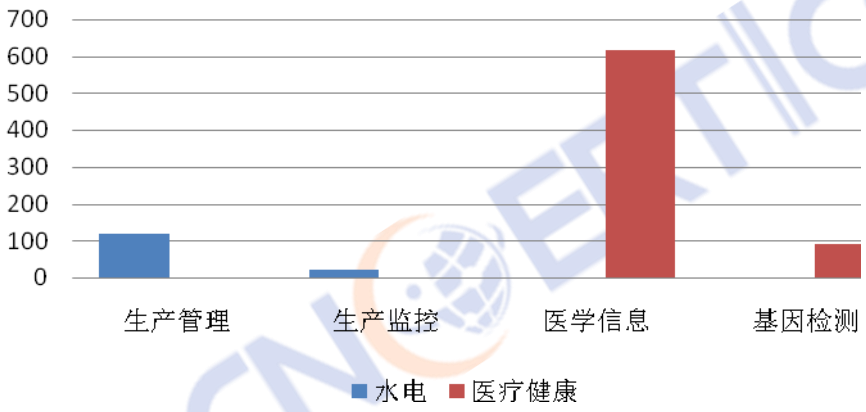

图 10 2019 年上半年发现的重点行业联网监控管理系统分类

（七）互联网金融安全

为实现对我国互联网金融平台网络安全总体态势的宏观监测，CNCERT 发挥技术优势，建设了国家互联网金融风

险分析技术平台网络安全监测功能，对我国互联网金融相关网站、移动 APP 等的安全风险进行监测。

1. 互联网金融网站安全情况

2019 年上半年，CNCERT 监测发现互联网金融网站的高危漏洞 92 个，其中 SQL 注入漏洞 27 个（占比 29.3%）；其次是远程代码执行漏洞 20 个（占比 21.7%）和敏感信息泄漏漏洞 16 个（占比 17.4%），如图 11 所示。近年来，随着互联网金融行业的发展，互联网金融平台运营者的网络安全意识有所提升，互联网金融平台的网络安全防护能力有所加强，特别是规模较大的平台，但仍有部分平台安全防护能力不足，安全隐患较多。

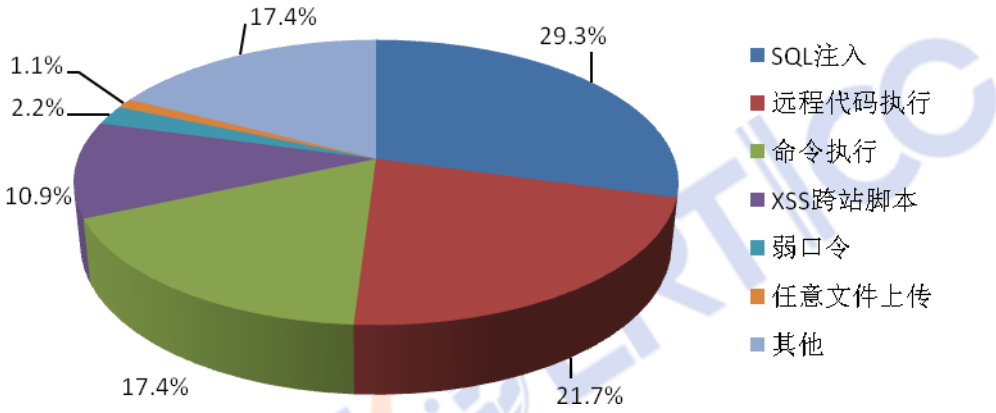

图 11 互联网金融网站高危漏洞分布情况

2. 互联网金融 APP 安全情况

在移动互联网技术发展和应用普及的背景下，用户通过互联网金融 APP 进行投融资的活动愈加频繁，绝大多数的互联网金融平台通过移动 APP 开展业务，且有部分平台仅通过

移动 APP 开展业务。2019 年上半年，CNCERT 对 105 款互联网金融 APP 进行检测，发现安全漏洞 505 个，其中高危漏洞 239 个。在这些高危漏洞中，明文数据传输漏洞数量最多有 59 个（占高危漏洞数量的 24.7%），其次是网页视图（Webview）明文存储密码漏洞有 58 个（占 24.3%）和源代码反编译漏洞有 40 个（占 16.7%），如图 12 所示。这些安全漏洞可能威胁交易授权和数据保护，存在数据泄露风险，其中部分安全漏洞影响应用程序的文件保护，不能有效阻止应用程序被逆向或者反编译，进而使应用暴露出多种安全风险。

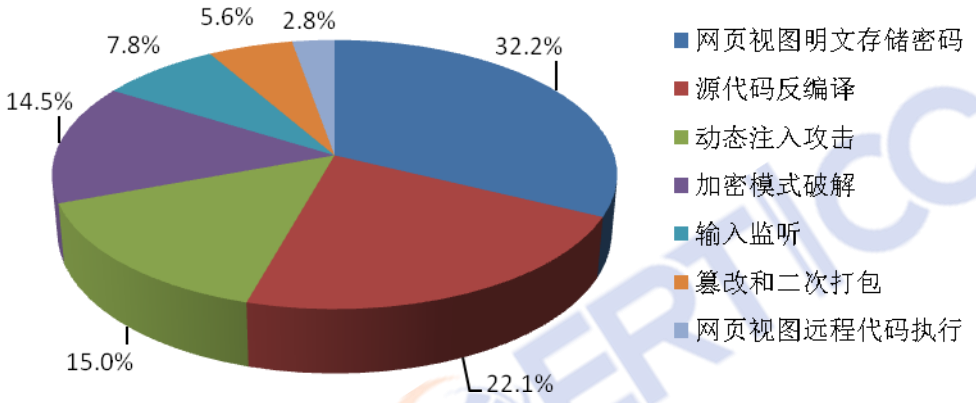

图 12 互联网金融移动 APP 高危漏洞分布情况

二、2019 年上半年我国互联网网络安全状况特点

（一）个人信息和重要数据泄露风险严峻

2019 年初，在我国境内大量使用的 MongoDB、

Elasticsearch 数据库相继曝出存在严重安全漏洞，可能导致数据泄露风险，凸显了我国数据安全问题严重。CNCERT 抽样监测发现，我国境内互联网上用于 MongoDB 数据库服务的 IP 地址约 2.5 万个，其中存在数据泄露风险的 IP 地址超过 3,000 个，涉及我国一些重要行业。Elasticsearch 数据库也曝出类似安全隐患。经过分析，CNCERT 发现这两个数据库均是在默认情况下，无需权限验证即可通过默认端口本地或远程访问数据库并进行任意的增、删、改、查等操作。在数据库启用连接公共互联网前，用户需做好相关安全设置以及数据库访问安全策略，才能有效避免数据泄露风险。

（二）多个高危漏洞曝出给我国网络安全造成严重安全隐患

2019 年以来，WinRAR 压缩包管理软件、Microsoft 远程桌面服务、Oracle WebLogic wls-9-async 组件等曝出存在远程代码执行漏洞[⑤]，给我国网络安全造成严重安全隐患。以 Oracle WebLogicwls-9-async 组件存在反序列化远程命令执行“零日”漏洞为例，该漏洞容易利用，攻击者利用该漏洞可对目标网站发起植入后门、网页篡改等远程攻击操作，对我国网络安全构成了较为严重的安全隐患。这些基础软件广泛应用在我国基础应用和通用软硬件产品中，若未得到及时

[⑤] 对应的 CNVD 编号：WinRAR 系列任意代码执行漏洞（CNVD-2019-04911、CNVD-2019-04912、CNVD-2019-04913 与 CNVD-2019-04910），Microsoft 远程桌面服务远程代码执行漏洞（CNVD-2019-14264），Oracle WebLogic wls9-async 反序列化远程命令执行漏洞（CNVD-C-2019-48814）。

修复，容易遭批量利用，造成严重危害。同时，近年来“零日”漏洞收录数量持续走高，在 2019 年上半年 CNVD 收录的通用型安全漏洞数量中，“零日”漏洞收录数量占比 43.3%，同比增长 34.0%，因这些漏洞在披露时尚未发布补丁或相应的应急策略，一旦被恶意利用，将可能产生严重安全威胁。针对安全漏洞可能产生的危害，CNVD 持续加强对重大高危漏洞的应急处置协调，2019 年上半年通报安全漏洞事件万余起。

（三）针对我国重要网站的 DDoS 攻击事件高发

正像前期预测，2019 年具有特殊目的针对性更强的网络攻击越来越多。2019 年上半年，CNCERT 监测发现针对我国重要网站的 CC 攻击事件高发。攻击者利用公开代理服务器向目标网站发起大量的访问，访问内容包括不存在的页面、网站大文件、动态页面等，由此来绕过网站配置的 CDN 节点直接对网站源站进行攻击，达到了使用较少攻击资源造成目标网站访问缓慢甚至瘫痪的目的。2019 年上半年，CNCERT 抽样监测发现，针对我国境内目标的 DDoS 攻击中，来自境外的 DDoS 攻击方式以 UDP Amplification FLOOD 攻击、TCP SYN FLOOD 攻击方式等为主，其中又以 UDP Amplification FLOOD 攻击方式占比最高约 75%。

（四）利用钓鱼邮件发起有针对性的攻击频发

2019 年上半年，CNCERT 监测发现恶意电子邮件数量超

过 5600 万封，涉及恶意邮件附件 37 万余个，平均每个恶意电子邮件附件传播次数约 151 次。钓鱼邮件一般是攻击者伪装成同事、合作伙伴、朋友、家人等用户信任的人，通过发送电子邮件的方式，诱使用户回复邮件、点击嵌入邮件正文的恶意链接或者打开邮件附件以植入木马或间谍程序，进而窃取用户敏感数据、个人银行账户和密码等信息，或者在设备上执行恶意代码实施进一步的网络攻击活动，因欺骗迷惑性很强，用户稍不谨慎就很容易上当。其中，对通过钓鱼邮件窃取邮箱账号密码情况进行分析，CNCERT 监测发现我国平均每月约数万个电子邮箱账号密码被攻击者窃取，攻击者通过控制这些电子邮件对外发起攻击。例如 2019 年初，某经济黑客组织利用我国数百个电子邮箱对其他国家的商业和金融机构发起钓鱼攻击。

三、2019 年上半年网络安全威胁治理工作开展情况

2019 年上半年，CNCERT 协调处置网络安全事件约 4.9 万起，同比减少 7.7%，其中安全漏洞事件最多，其次是恶意程序、网页仿冒、网站后门、网页篡改、DDoS 攻击等事件。此外，2019 年以来，我国有关部门针对移动应用违法违规收集使用个人信息、互联网网站安全等开展专项治理工作，以规范市场秩序、维护我国网络安全。

（一）我国网络安全治理的顶层设计逐步完善

近年来，我国用户个人信息和重要数据保护工作受到广

泛关注，我国正在抓紧推进数据保护方面的规章制度、标准等的制定工作。2019 年以来，国家互联网信息办公室会同各行业主管部门研究起草了《数据安全管理办法（征求意见稿）》、《网络安全审查办法（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》、《儿童个人信息网络保护规定（征求意见稿）》、《APP 违法违规收集使用个人信息行为认定方法（征求意见稿）》，并面向社会公开征求意见。此外，为规范网络安全漏洞报告和信息发布等行为，保证网络产品、服务、系统的漏洞得到及时修补，提高网络安全防护水平，工业和信息化部会同有关部门起草了规范性文件《网络安全漏洞管理规定（征求意见稿）》，正在向社会公开征求意见。

（二）移动 APP 违规收集个人信息治理专项

随着移动互联网技术的快速发展和应用，移动互联网终端应用已成为互联网用户上网的首要入口和互联网信息服务的主要形式。根据统计，我国境内应用商店数量已超过 200 家，上架应用近 500 万款，下载总量超过万亿次，发展势头迅猛。与此同时，移动 APP 强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，广大网民对此反应强烈。CNCERT 监测分析发现，在目前下载量较大的千余款移动 APP 中，每款应用平均申请 25 项权限，其中申请了与业务无关的拨打电话权限的 APP

数量占比超过 30%；每款应用平均收集 20 项个人信息和设备信息，包括社交、出行、招聘、办公、影音等；大量 APP 存在探测其他 APP 或读写用户设备文件等异常行为，对用户的个人信息安全造成潜在安全威胁。为保障个人信息安全，维护广大网民合法权益，中央网信办、工业和信息化部、公安部、市场监管总局决定，2019 年在全国范围组织开展 APP 违法违规收集使用个人信息专项治理，组织开展移动应用专项评估。专项治理工作启动以来，多项成果文件向社会发布，包括《百款常用 APP 强制开启权限情况通报》、《网络安全实践指南——移动互联网应用基本业务功能必要信息规范》、《APP 违法违规收集使用个人信息行为认定办法》等，有效指导 APP 运营者加强个人信息保护，规范市场秩序。

（三）互联网网站安全整治专项

2019 年 5 月至 12 月，中央网信办、工业和信息化部、公安部、市场监管总局四部门联合开展全国范围的互联网网络安全专项整治工作。专项整治工作将对未备案或备案信息不准确的网站进行清理，对攻击网站的违法犯罪行为进行严厉打击，对违法违规网站进行处罚和公开曝光。此次专项整治的一大特点是将加大对未履行网络安全义务、发生事件的网站运营者的处罚力度，督促其切实落实安全防护责任，加强网站安全管理和维护。专项整治期间，中央网信办将加强统筹协调，指导有关部门做好信息共享、协同配合，坚持依

法依规，坚持防摄并举，促使网站运营者网络安全意识和防护能力有效提升，实现网站安全形势取得明显改观。截至2019年6月，互联网网站安全专项整治行动期间，共享网站安全事件511起，其中网页篡改事件占比最高达89.2%。

（四）DDoS攻击团伙治理工作

2019年以来，CNCERT持续开展DDoS攻击团伙的追踪和治理工作，截至目前，2018年活跃的较大规模DDoS攻击团伙[⑥]大部分已不再活跃，但有5个攻击团伙通过不断变换资源持续活跃。其中最活跃的攻击团伙主要使用XorDDoS僵尸网络发起DDoS攻击，惯常使用包含特定字符串的恶意域名对僵尸网络进行控制，对游戏私服、色情、赌博等相关的服务器发起攻击。分析发现，恶意域名大多在境外域名注册商注册，并通过不断变换控制端IP地址，持续活跃对外发起大量攻击。

2019年上半年，我国迎来了5G商用牌照正式发放，我国互联网的发展又进入了一个新时期。5G技术将加速更多行业的数字化转型，拓展大市场，带来新机遇，有力支撑数字经济蓬勃发展。与此同时，也预示互联网上承载的信息将更为丰富，物联网将大规模发展。但用户个人信息和重要数据泄露风险严峻、有针对性的攻击行动频发等情况，严重威胁我国网络空间安全。预计在2019年下半年，保护用户个

⑥ CNCERT发布的《2018年活跃DDoS攻击团伙分析报告》

人信息和重要数据安全、有效治理和防范网络攻击、全面研究新技术新业务应用带来的安全风险等方面仍然是我们要重点关注的方向。