2020年上半年我国互联网网络安全监测数据分析报告

国家计算机网络应急技术处理协调中心

2020年9月

目　录

为全面反映 2020 年上半年我国互联网在恶意程序传播、漏洞风险、DDoS 攻击、网站安全等方面的情况，CNCERT 对上半年监测数据进行了梳理，形成监测数据分析报告如下。

一、恶意程序

（一）计算机恶意程序捕获情况

2020 年上半年，捕获计算机恶意程序样本数量约 1,815 万个，日均传播次数达 483 万余次，涉及计算机恶意程序家族约 1.1 万余个。按照传播来源统计，境外恶意程序主要来自美国、塞舌尔和加拿大等，境外具体分布如图 1 所示；位于境内的恶意程序主要来自浙江省、广东省和北京市等。按照目标 IP 统计，我国境内受计算机恶意程序攻击的 IP 地址约 4,208 万个，约占我国 IP 总数的 12.4%，这些受攻击的 IP 地址主要集中在山东省、江苏省、广东省、浙江省等，我国受计算机恶意程序攻击的 IP 分布情况如图 2 所示。

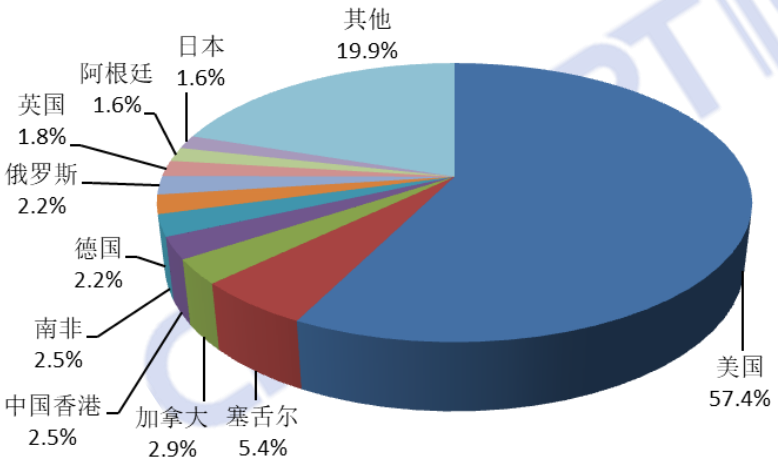

图 1 计算机恶意代码传播源位于境外分布情况

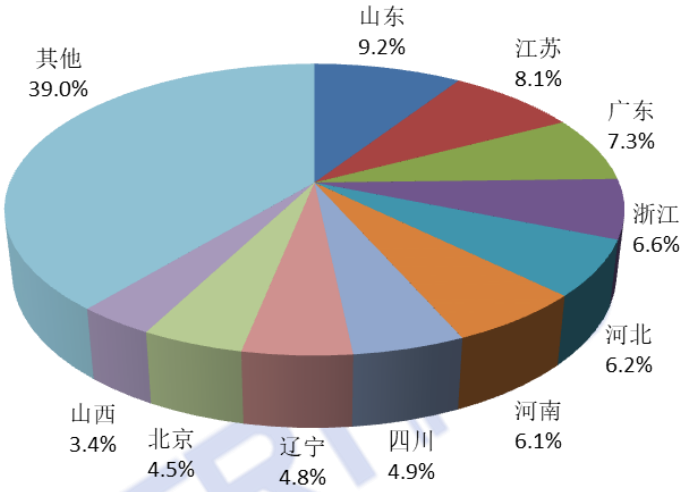

图 2 我国受计算机恶意代码攻击的 IP 分布情况

（二）计算机恶意程序用户感染情况

我国境内感染计算机恶意程序的主机数量约 304 万台，同比增长 25.7%。位于境外的约 2.5 万个计算机恶意程序控制服务器控制我国境内约 303 万台主机。就控制服务器所属国家或地区来看，位于美国、中国香港地区和荷兰的控制服务器数量分列前三位，分别是约 8,216 个、1,478 个和 1,064 个，具体分布如图 3 所示；就所控制我国境内主机数量来看，位于美国、荷兰和德国的控制服务器控制规模分列前三位，分别控制我国境内约 252 万、127 万和 117 万台主机，如图 4 所示。此外，根据抽样监测数据发现，针对 IPv6 网络的攻击情况也开始出现，境外累计约 1,200 个 IPv6 地址的计算机恶意程序控制服务器控制了我国境内累计约 1.5 万台 IPv6 地址主机。

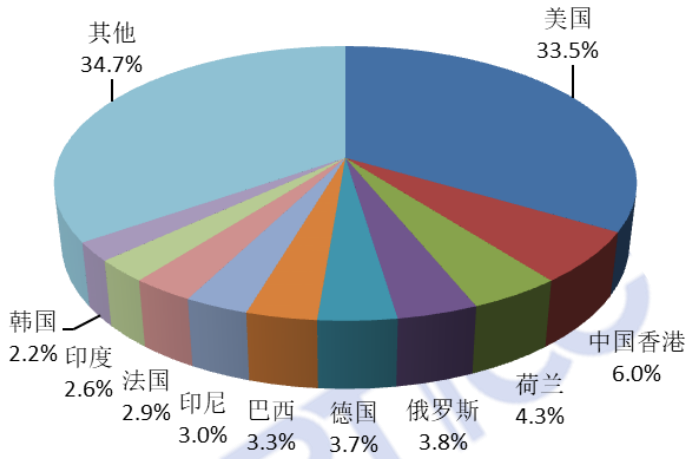

图 3 控制我国境内主机的境外木马僵尸网络控制端分布

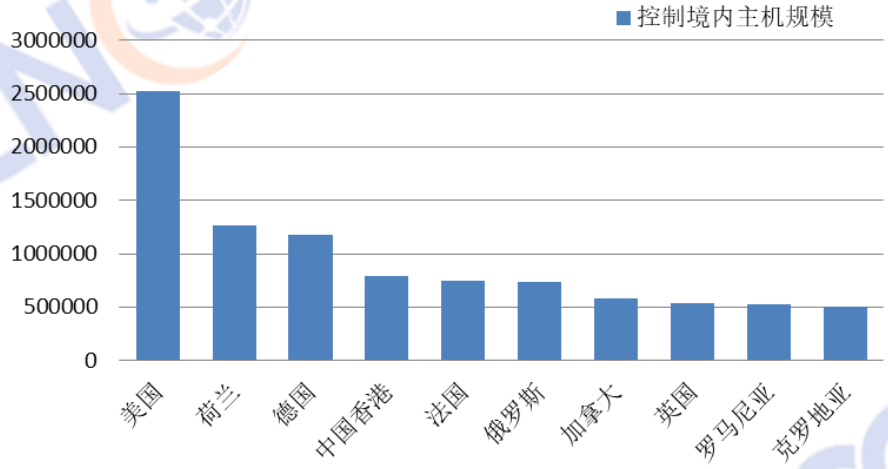

图 4 控制我国境内主机数量 TOP10 的国家或地区

从我国境内感染计算机恶意程序主机数量地区分布来看，主要分布在江苏省（占我国境内感染数量的 15.3%）、浙江省（占 11.9%）、广东省（占 11.6%）等，具体分布如图 5 所示。在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 4,696 个，规模在 10 万台以上的僵尸网络数量 16 个，如图 6 所示。相关机构处置了 45 个控制规模较大的僵尸网络，有效控制计算机恶意程序感染主机引发

的危害。

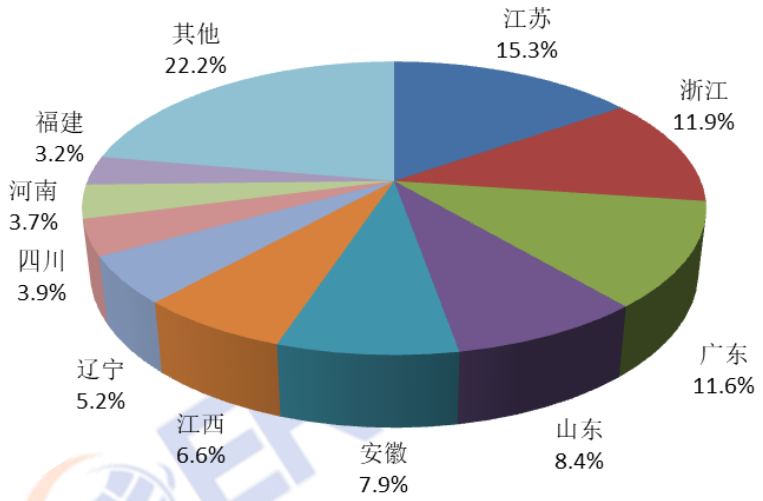

图 5 我国境内感染木马僵尸程序的主机数量按地区分布

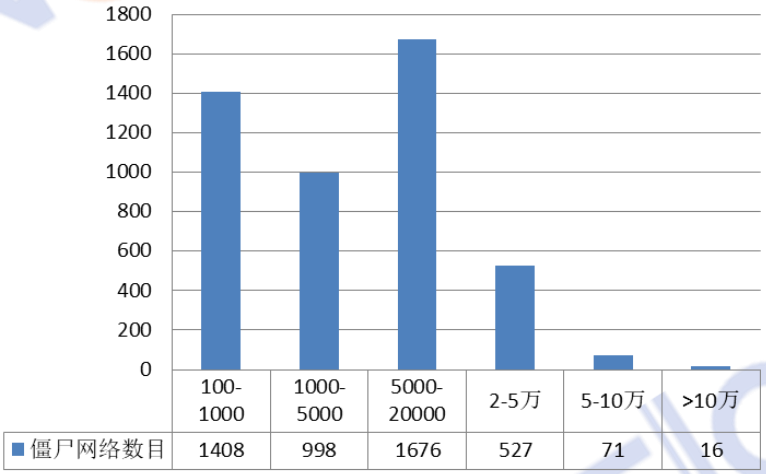

图 6 僵尸网络的规模分布

（三）移动互联网恶意程序

通过自主捕获和厂商交换发现新增移动互联网恶意程序 163 万余个，同比增长 58.3%。通过对恶意程序的恶意行为统计发现，排名前三的仍然是流氓行为类、资费消耗类和信息窃取类，占比分别为 36.5%、29.2%和 15.1%。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，国内 125 家提供移动应用程序下载服务的平台下架 812 个移动

互联网恶意程序，有效防范移动互联网恶意程序危害，严格控制移动互联网恶意程序传播途径。

近年来，我国逐步加大对应用商店、应用程序的安全管理力度，要求应用商店对上架 App 的开发者进行实名审核，对 App 进行安全检测和内容版权审核等，使得互联网黑产应用商店传播恶意 App 的难度明显增加。但同时，能够逃避监管并实现不良目的的“擦边球”式灰色应用却有所增长，例如：具有钓鱼目的、欺诈行为的仿冒 App 成为黑产的重要工具，持续对金融、交通、电信等重要行业的用户形成较大威胁。2020 年上半年，通过自主监测和投诉举报方式发现新出现的仿冒 App 下载链接 180 个。这些仿冒 App 具有容易复制、版本更新频繁、蹭热点快速传播等特点，主要集中在仿冒公检法、银行、社交软件、支付软件、抢票软件等热门应用上，仿冒方式以仿冒名称、图标、页面等内容为主，具有很强的欺骗性。目前，由于开发者在应用商店申请 App 上架前，需提交软件著作权等证明材料，因此仿冒 App 很难在应用商店上架，其流通渠道主要集中在网盘、云盘、广告平台等其他线上传播渠道。

（四）联网智能设备恶意程序

目前活跃在智能设备上的恶意程序家族超过 15 种，包括 Mirai、Gafgyt、Dofloo、Tsunami、Hajime、MrBlack、Mozi、PinkPot 等。这些恶意程序一般通过漏洞、暴力破解等途径入侵和控制智能设备。遭入侵控制后，联网智能设备存在用户信

息和设备数据被窃、硬件设备遭控制和破坏、设备被用作跳板对内攻击内网其他主机或对外发动 DDoS 攻击等安全威胁和风险。

上半年，发现智能设备恶意程序样本约 126 万余个，其中大部分属于 Mirai 家族和 Gafgyt 家族，占比超过 96.0%。服务端传播源 IP 地址 5 万余个，我国境内疑似受感染智能设备 IP 地址数量约 92 万个，与 2019 上半年相比基本持平，主要位于浙江省、江苏省、安徽省、山东省、辽宁省等地。被控联网智能设备日均向 1 千余个目标发起 DDoS 攻击，与 2019 年上半年相比也基本持平。

二、安全漏洞

国家信息安全漏洞共享平台（CNVD）收录通用型安全漏洞 11,073 个，同比大幅增长 89.0%。其中，高危漏洞收录数量为 4,280 个（占 38.7%），同比大幅增长 108.3%，“零日”漏洞收录数量为 4,582 个（占 41.4%），同比大幅增长 80.7%。安全漏洞主要涵盖的厂商或平台为谷歌（Google）、WordPress、甲骨文（Oracle）等。按影响对象分类统计，排名前三的是应用程序漏洞（占 48.5%）、Web 应用漏洞（占 26.5%）、操作系统漏洞（占 10.0%），如图 7 所示。2020 年上半年，CNVD 处置涉及政府机构、重要信息系统等网络安全漏洞事件近 1.5 万起。

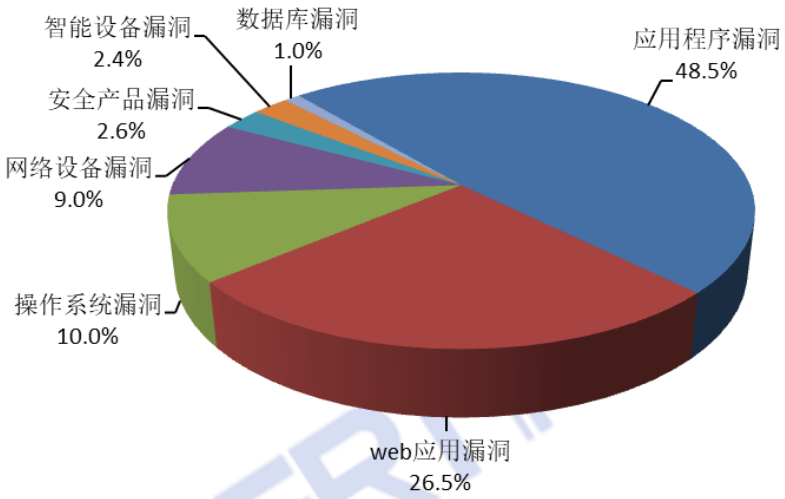

图 7 CNVD 收录安全漏洞按影响对象分类统计

三、拒绝服务攻击

因攻击成本低、攻击效果明显等特点，DDoS 攻击仍然是互联网用户面临的最常见、影响较大的网络安全威胁之一。抽样监测发现，我国每日峰值流量超过 10Gbps 的大流量 DDoS 攻击事件数量与 2019 年基本持平，约 220 起。

（一）攻击资源活跃情况

经过持续监测分析与处置，可被利用的 DDoS 攻击资源稳定性降低，可利用活跃资源数量被控制在较低水平。累计监测发现用于发起 DDoS 攻击的活跃 C&C 控制服务器 2,379 台，其中位于境外的占比 95.5%，主要来自美国、荷兰、德国等；活跃的受控主机约 122 万台，其中来自境内的占比 90.3%，主要来自江苏省、广东省、浙江省、山东省、安徽省等；反射攻击服务器约 801 万台，其中来自境内的占比 67.4%，主要来自辽宁省、浙江省、广东省、吉林省、黑龙江省等。

（二）境内大流量攻击情况

在监测发现境内峰值流量超过 10Gbps 的大流量攻击事件中，主要攻击方式仍然是 TCP SYN Flood、NTP Amplification、SSDP Amplification、DNS Amplification 和 UDP Flood，以上五种攻击占比达到 82.9%。为躲避溯源，攻击者倾向于使用这些便于隐藏攻击源的攻击方式，并会根据攻击目标防护情况灵活组合攻击流量，混合型攻击方式占比为 16.4%。此外，随着近年来“DDoS 即服务”黑产模式猖獗，攻击者倾向于使用大流量攻击将攻击目标网络瞬间瘫痪，DDoS 攻击时长小于半小时的攻击占比达 81.5%，攻击目标主要位于浙江省、江苏省、福建省、山东省、广东省、北京市等，占比高达 81.1%。

（三）主流攻击平台活跃情况

通过持续监测和跟踪 DDoS 攻击平台活跃情况发现，网页 DDoS 攻击平台以及利用 Gafgyt、Mirai、Xor、BillGates、Mayday 等僵尸网络家族发起攻击仍持续活跃，发起 DDoS 攻击事件较多。作为“DDoS 即服务”黑产模式之一的网页 DDoS 攻击平台，因其直接面向用户提供服务，可由用户按需自主发起攻击，极大降低了发起 DDoS 攻击难度，导致 DDoS 攻击进一步泛滥。监测发现，由网页 DDoS 攻击平台发起的 DDoS 攻击事件数量最多，同比 2019 年上半年增加 32.2%。当前互联网上大量活跃的缺乏安全防护的物联网设备，为 DDoS 攻击平台猖獗发展提供了大量被控资源，导致 DDoS 攻击事件一直高居不下。

Gafgyt 和 Mirai 恶意程序新变种不断出现，使得利用其形成的僵尸网络控制端和攻击事件数量维持在较高水平，而 Xor 恶意程序家族有明显特征显示其在对外提供“DDoS 即服务”黑产业务，表现出以少量控制端维持较高攻击频度。

四、网站安全

（一）网页仿冒

监测发现针对我国境内网站仿冒页面约 1.9 万个。CNCERT 重点针对金融行业、电信行业网上营业厅等 6,226 个仿冒页面进行处置，同比减少 48.1%。在已协调处置的仿冒页面中，承载仿冒页面 IP 地址归属地居首位仍然是中国香港地区，占比达 74.0%。

同时，互联网上关于“ETC 在线认证”网站的仿冒页面数量呈井喷式增长。进入 5 月后，在针对我国境内网站的仿冒页面中，涉及“ETC 在线认证”相关的网页仿冒数量占比高达 61.2%，此类钓鱼网站的主要承载 IP 地址仍然位于境外。仿冒形式主要包括“ETC 信息认证”“ETC 在线办理认证”“ETC 在线认证中心”等不同页面主题，诈骗分子诱骗用户提交真实姓名、银行卡账号、身份证号、银行预留手机号、取款密码等个人隐私信息。

（二）网站后门

境内外约 1.8 万个 IP 地址对我国境内约 3.59 万个网站植入后门，我国境内被植入后门的网站数量较 2019 年上半年增

长 36.9%。其中，约有 1.8 万个境外 IP 地址（占全部 IP 地址总数的 99.3%）对境内约 3.57 万个网站植入后门，位于美国的 IP 地址最多，占境外 IP 地址总数的 19.0%，其次是位于菲律宾和中国香港地区的 IP 地址，如图 8 所示。从控制我国境内网站总数来看，位于菲律宾的 IP 地址控制我国境内网站数量最多，约为 1.36 万个，其次是位于中国香港地区和美国的 IP 地址，分别控制我国境内 7,300 个和 6,020 个网站。此外，随着我国 IPv6 规模部署工作加速推进，支持 IPv6 的网站范围不断扩大。此外，攻击源、攻击目标为 IPv6 地址的网站后门事件 592 起，共涉及攻击源 IPv6 地址累计 35 个、被攻击 IPv6 地址解析网站域名累计 72 个。

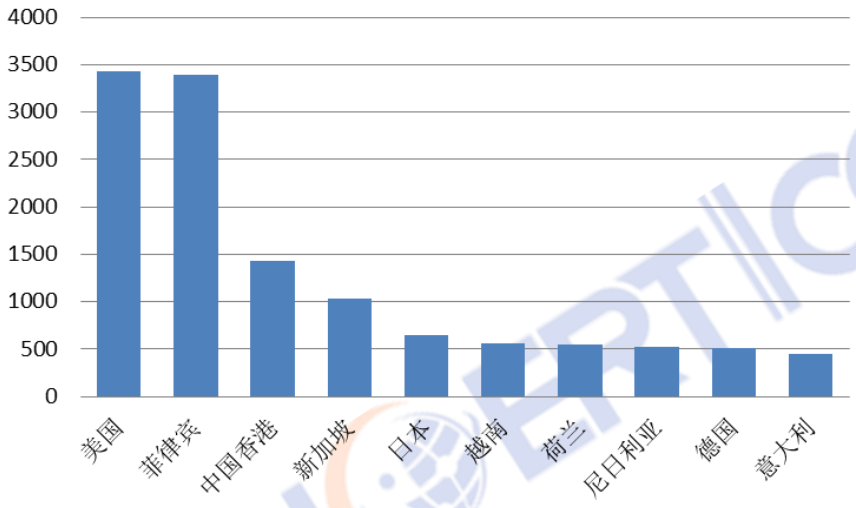

图 8 境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

（三）网页篡改

我国境内遭篡改的网站有约 7.4 万个，其中被篡改的政府网站有 318 个。从境内被篡改网页的顶级域名分布来看，占比

分列前三位的仍然是“.com”“.net”和“.org”，分别占总数的 74.1%、5.1%和 1.7%，如图 9 所示。

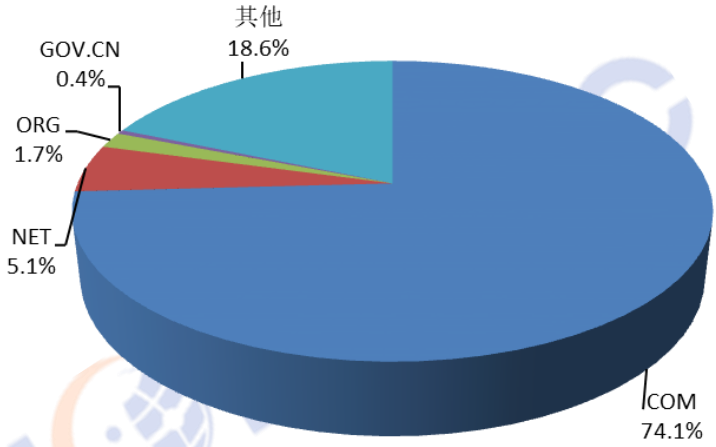

图 9 境内被篡改网站按顶级域名分布

五、云平台安全

我国云平台上网络安全威胁形势依然较为严峻。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 76.1%、被植入后门链接数量占境内全部被植入后门链接数量的 90.3%、被篡改网页数量占境内被篡改网页数量的 93.2%。其次，攻击者经常利用我国云平台发起网络攻击。其中云平台作为控制端发起 DDoS 攻击次数占境内控制发起 DDoS 攻击次数的 79.0%，作为木马和僵尸网络恶意程序控制的被控端 IP 地址数量占境内全部被控端 IP 地址数量的 96.3%，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 79.0%。

六、工业控制系统安全

（一）工业控制系统互联网侧暴露情况

监测发现暴露在互联网上的工业设备达 4,630 台，涉及国内外 35 家厂商的可编程逻辑控制器、智能楼宇、数据采集等 47 种设备类型，具体类型分布如图 10 所示。其中存在高危漏洞隐患的设备占比约 41%。监测发现电力、石油天然气、城市轨道交通等重点行业暴露的联网监控管理系统 480 套，其中电力 262 套、石油天然气 118 套、城市轨道交通 100 套，涉及的类型包括政府监管平台、远程监控、资产管理、工程安全、数据检测系统、管网调度系统、OA 系统、云平台等，具体平台类型分布如图 11 所示。其中存在信息泄露、跨站请求伪造、输入验证不当等高危漏洞隐患的系统占比约 11.1%。暴露在互联网的工业控制系统一旦被攻击，将严重威胁生产系统的安全。

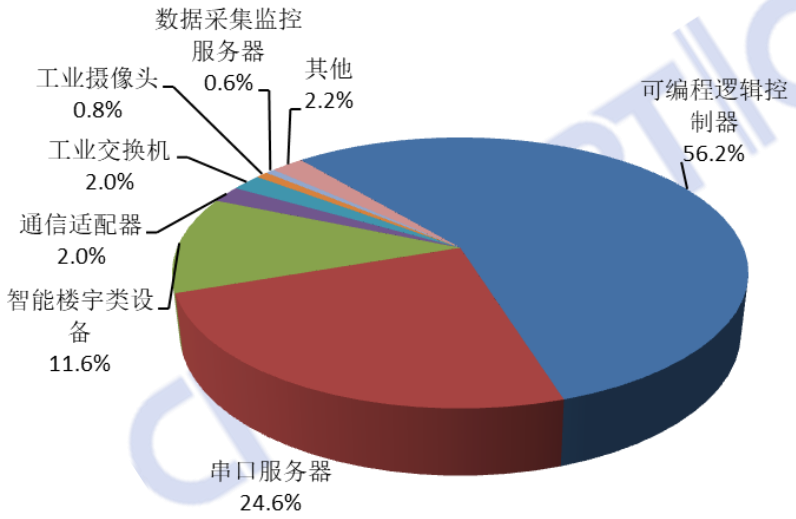

图 10 监测发现的联网工业设备的类型统计

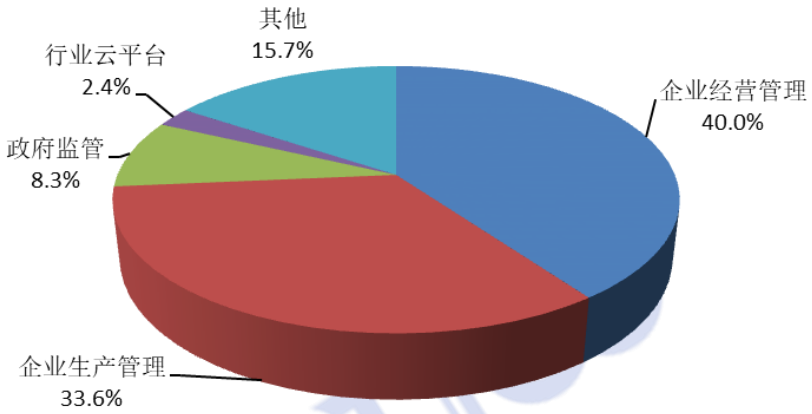

图 11 监测发现的重点行业联网监控管理系统类型统计

（二）工业控制系统互联网侧威胁监测情况

境内工业控制系统的网络资产持续遭受来自境外的扫描嗅探，日均超过 2 万次。经分析，嗅探行为源自于美国、英国、德国等境外 90 个国家，目标涉及境内能源、制造、通信等重点行业的联网工业控制设备和系统。大量关键信息基础设施及其联网控制系统的网络资产信息被境外嗅探，给我国网络空间安全带来隐患。

我国根云、航天云网、OneNET、COSMOPlat、奥普云、机智云等大型工业云平台持续遭受来自境外的网络攻击，平均攻击次数 114 次/日，同比上升 27%，攻击类型如图 12 所示，涉及远程代码执行、拒绝服务、Web 漏洞利用等，工业云平台承载着大量接入设备、业务系统，以及企业、个人信息和重要数据，使其成为网络攻击的重点目标。

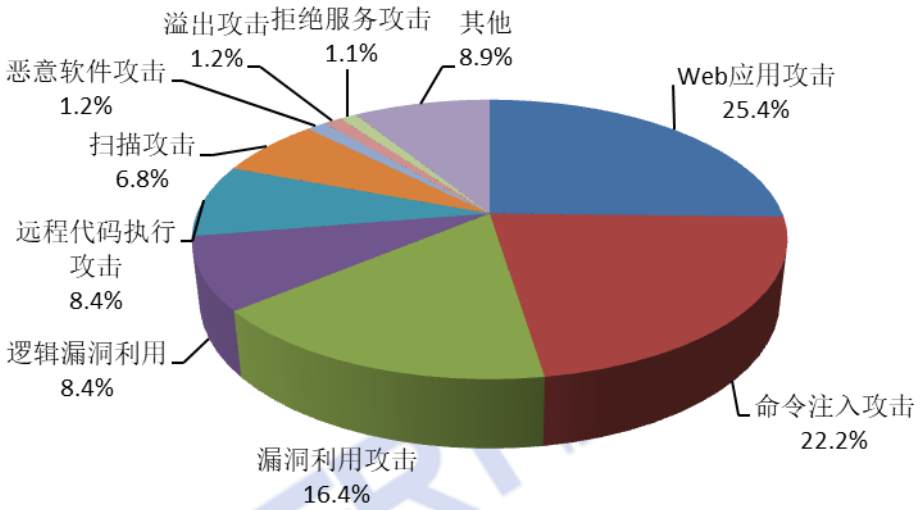

图 12 工业云平台攻击事件的类型分布

（三）工业控制产品安全漏洞情况

CNVD、CVE、NVD 及 CNNVD 四大漏洞平台新增收录工业控制系统产品漏洞共计 323 个，其中高中危漏洞占比达 94.7%。如图 13 和图 14 所示，漏洞影响的产品广泛应用于制造业、能源、水处理、信息技术、化工、交通运输、商业设施、农业、水利工程、政府机关等关键信息基础设施行业，漏洞涉及的产品供应商主要包括 ABB、万可、西门子、研华、施耐德、摩莎、三菱、海为、亚控、永宏等。

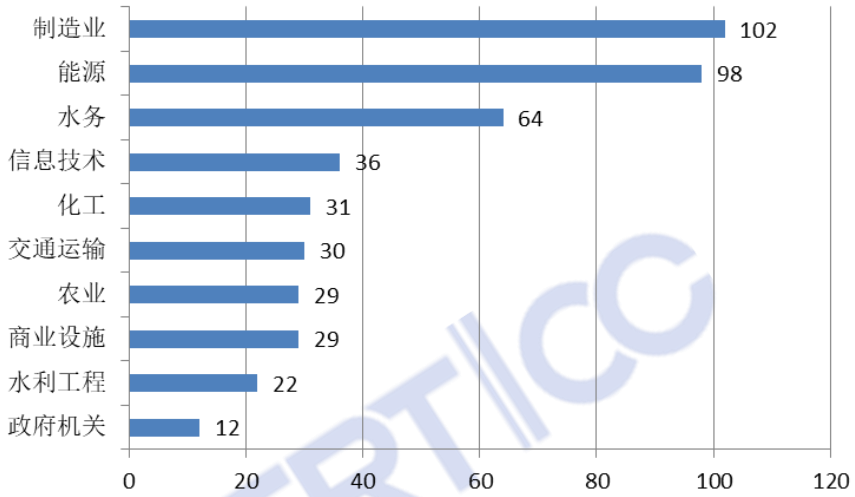

图 13 新增工业控制产品漏洞的行业分布 TOP10

（注：受漏洞影响的产品可应用于多个行业）

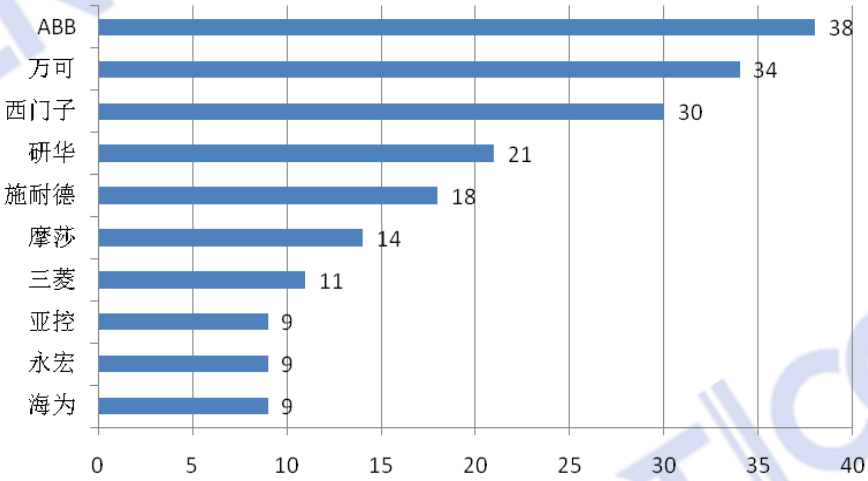

图 14 新增工业控制产品漏洞的供应商分布 TOP10