2021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

2021年7月

目　录

为全面反映 2021 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）恶意程序捕获情况

2021 年上半年，捕获恶意程序样本数量约 2,307 万个，日均传播次数达 582 万余次，涉及恶意程序家族约 20.8 万个。按照传播来源统计，境外来源主要来自美国、印度和日本等，具体分布如图 1 所示；境内来源主要来自河南省、广东省和浙江省等。按照攻击目标 IP 地址统计，我国境内受恶意程序攻击的 IP 地址近 3,048 万个，约占我国 IP 地址总数的 7.8%，这些受攻击的 IP 地址主要集中在广东省、江苏省、浙江省等地区，我国受恶意程序攻击的 IP 地址分布情况如图 2 所示。

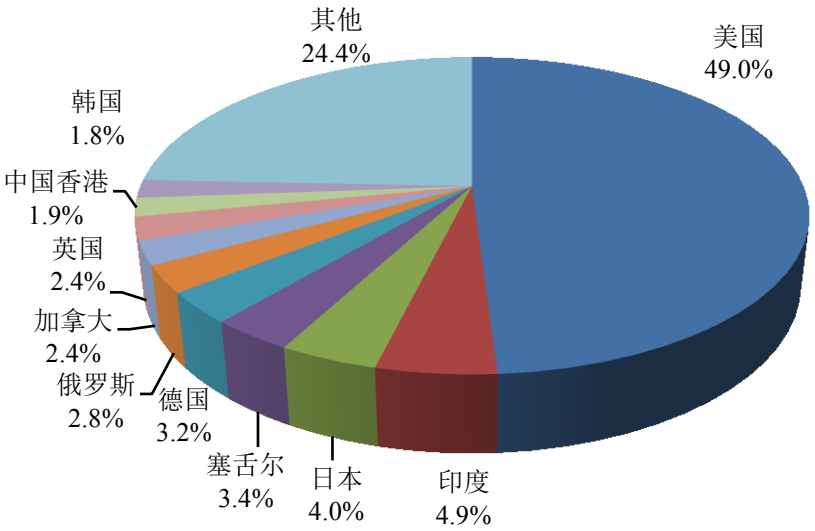

图 1 恶意程序传播源位于境外分布情况

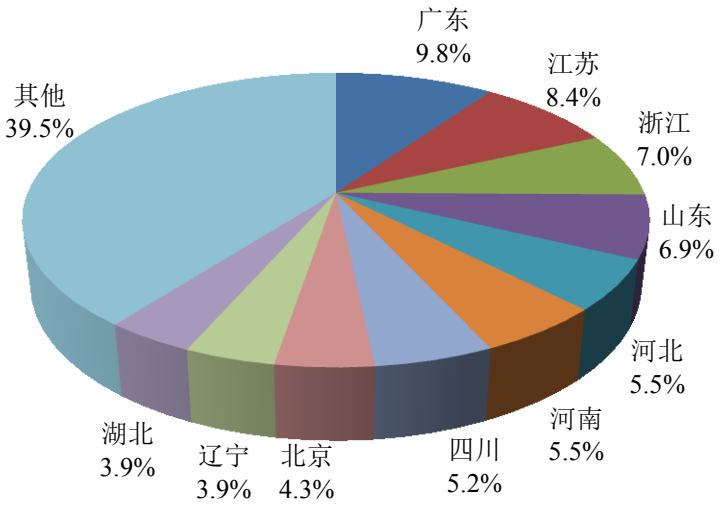

图 2 我国受恶意程序攻击的 IP 分布情况

（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 446 万台，同比增长 46.8%。位于境外的约 4.9 万个计算机恶意程序控制服务器控制我国境内约 410 万台主机。就控制服务器所属国家或地区来看，位于美国、越南和中国香港地区的控制服务器数量分列前三位，分别是约 7,580 个、3,752 个和 2,451 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、中国香港地区和荷兰的控制服务器控制规模分列前三位，分别控制我国境内约 314.5 万、118.9 万和 108.6 万台主机，如图 4 所示。此外，根据 CNCERT 抽样监测数据，境外约 1.2 万个 IPv6 地址控制了我国境内约 2.3 万台 IPv6 地址主机。

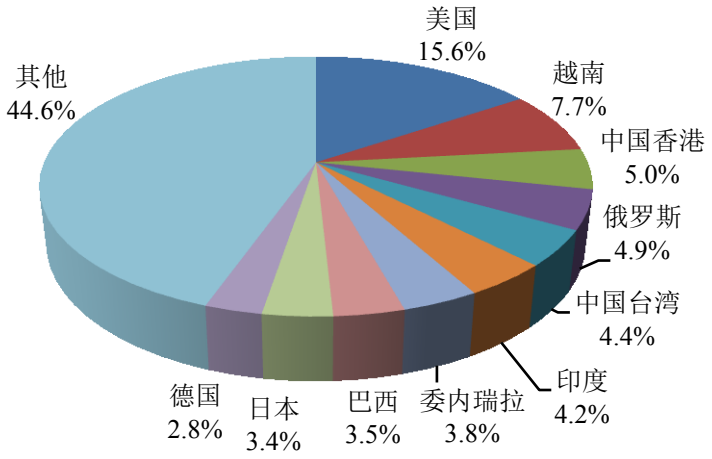

图 3 控制我国境内主机的境外计算机恶意程序控制服务器数量分布

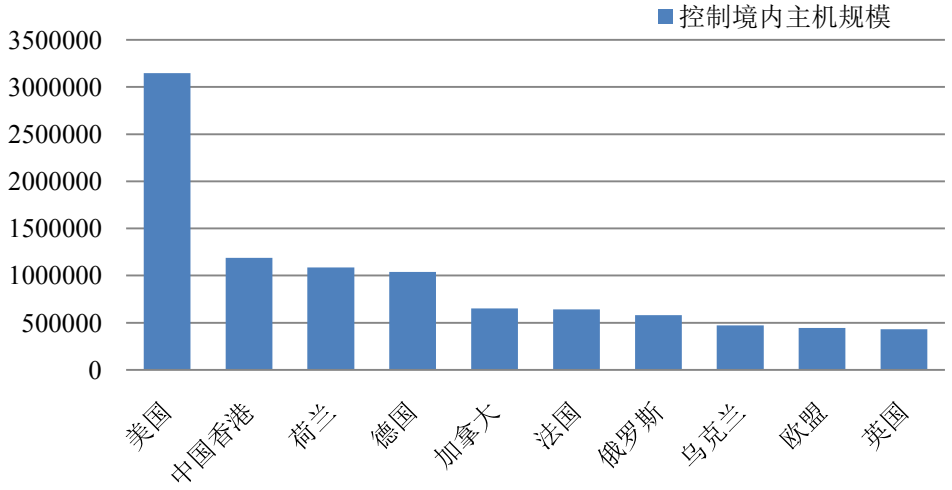

图 4 控制我国境内主机数量 TOP10 的国家或地区

从我国境内感染计算机恶意程序主机所属地区看，主要分布在广东省（占我国境内感染数量的 12.2%）、浙江省（占 11.0%）、江苏省（占 8.0%）等地区，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 2,307 个，规模在 10 万台以上的僵尸网络数量 68 个，如图 6 所示。CNCERT 协调相关机构成功关闭 259 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。

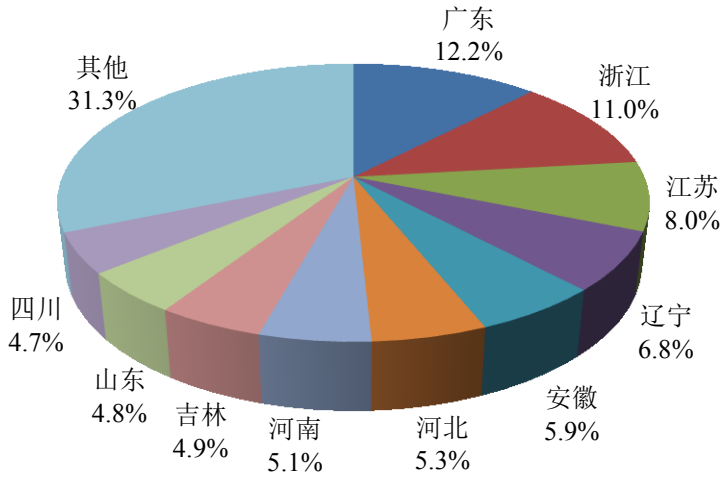

图 5 我国境内感染计算机恶意程序主机数量按地区分布

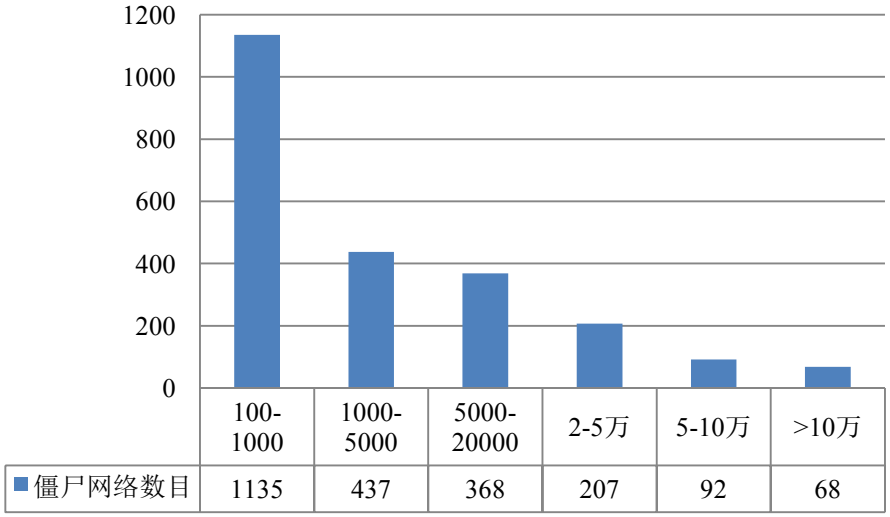

图 6 僵尸网络的规模分布

（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 86.6 万余个，同比下降 47.0%。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 47.9%、20.0%和 19.2%，如图 7 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，累计协调国内 204 家提供移动应用程序下

载服务的平台下架 25,054 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。

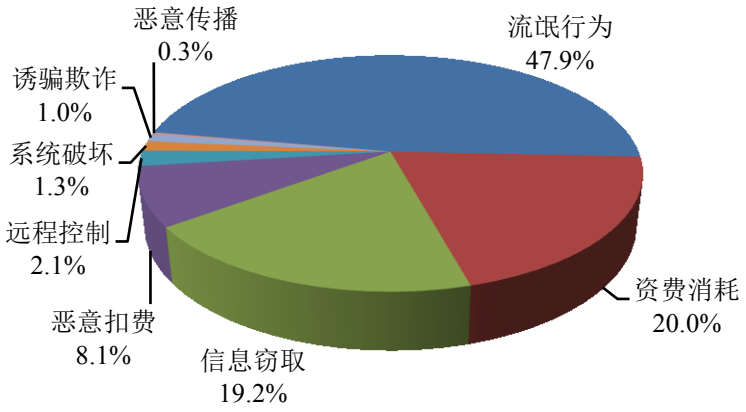

图 7 移动互联网恶意程序数量按行为属性统计

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 13,083 个，同比增长 18.2%。其中，高危漏洞收录数量为 3,719 个（占 28.4%），同比减少 13.1%；“零日”漏洞收录数量为 7,107 个（占 54.3%），同比大幅增长 55.1%。按影响对象分类统计，排名前三的是应用程序漏洞（占 46.6%）、Web 应用漏洞（占 29.6%）、操作系统漏洞（占 6.0%），如图 8 所示。2021 年上半年，CNVD 验证和处置涉及政府机构、重要信息系统等网络安全漏洞事件近 1.8 万起。

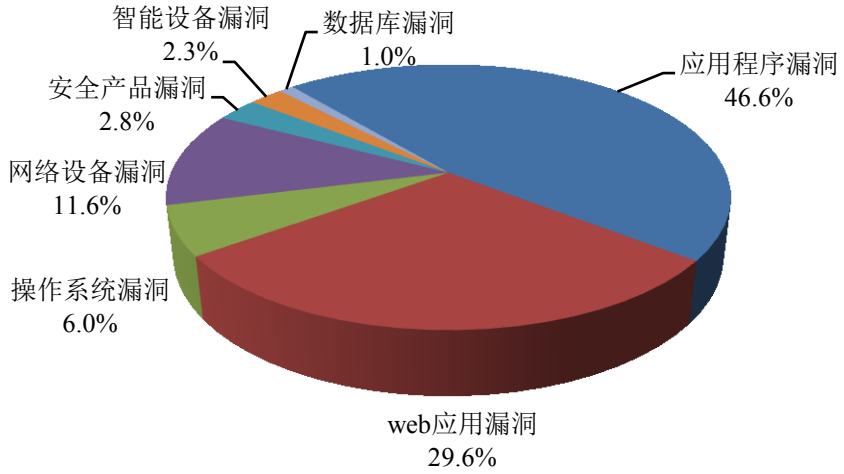

图 8 CNVD 收录安全漏洞按影响对象分类统计

三、拒绝服务攻击

为降低 DDoS 攻击对我国基础网络和关键信息基础设施的威胁，CNCERT 持续加强对境内目标遭大流量攻击情况的监测跟踪分析，针对所发现的被用于进行 DDoS 攻击的网络资源重点开展治理。

（一）境内目标遭大流量 DDoS 攻击情况

CNCERT 监测发现，境内目标遭受峰值流量超过 1Gbps 的大流量攻击事件同比减少 17.5%，主要攻击方式为 TCP SYN Flood、UDP Flood、NTP Amplification、DNS Amplification、TCP ACK Flood 和 SSDP Amplification，这 6 种攻击的事件占比达到 96.1%；攻击目标主要位于浙江省、山东省、江苏省、广东省、北京市、福建省、上海市等地区，这 7 个地区的事件占比达到 81.7%；1 月份是上半年攻击最高峰，攻击较为活跃；攻击时长不超过 30 分钟的攻击事件占比高达 96.6%，比例进一步上升，表明攻击者越来越倾向于利用大流量攻击瞬间打瘫

攻击目标。

（二）被用于进行 DDoS 攻击的网络资源活跃情况

CNCERT 通过开展对境内目标遭大流量 DDoS 攻击事件的持续分析溯源，发布《我国 DDoS 攻击资源季度分析报告》，定期公布控制端、被控端、反射服务器、伪造流量来源路由器等被用于进行 DDoS 攻击的网络资源（以下简称“攻击资源”）情况，并进一步协调各单位处置，境内可被利用的攻击资源稳定性继续降低，被利用的活跃境内攻击资源数量控制在较低水平。累计监测发现用于发起 DDoS 攻击的活跃控制端 1,455 台，其中位于境外的占比 97.1%，主要来自美国、德国和荷兰等；活跃肉鸡 71 万余台，其中位于境内的占比 92.7%，主要来自广东省、辽宁省、江苏省、福建省、浙江省等；反射攻击服务器约 395 万余台，其中位于境内的占比 80.7%，主要来自浙江省、广东省、辽宁省、吉林省、四川省等。与 2020 年上半年相比，境内各类攻击资源数量持续减少，境内活跃控制端数量同比减少 60.4%、肉鸡数量同比减少 40.1%、活跃反射服务器同比减少 40.9%。

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 1.3 万余个。为有效防止网页仿冒引发的危害，CNCERT 重点针对金融、电信等行业的仿冒页面进行处置，共协调关闭仿冒页面 8,171 个，

同比增加 31.2%。在已协调关闭的仿冒页面中，从承载仿冒页面 IP 地址归属情况来看，绝大多数位于境外。

监测发现，今年 2 月份以来，针对地方农信社的仿冒页面呈爆发趋势，仿冒对象不断变换转移，承载 IP 地址主要位于境外。这些仿冒页面频繁动态更换银行名称，多为新注册域名且通过伪基站发送钓鱼短信的方式进行传播。根据分析，通过此类仿冒页面，攻击者不仅仅可以获取受害人个人敏感信息，还可以冒用受害人身份登录其手机银行系统进行转账操作或者绑定第三方支付渠道进行资金盗取。

（二）网站后门

境内外 8,289 个 IP 地址对我国境内约 1.4 万个网站植入后门，我国境内被植入后门的网站数量较 2020 年上半年大幅减少 62.4%。其中，有 7,867 个境外 IP 地址（占全部 IP 地址总数的 94.9%）对境内约 1.3 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 15.8%，其次是位于菲律宾和中国香港地区的 IP 地址，如图 9 所示。从控制我国境内网站总数来看，位于中国香港地区的 IP 地址控制我国境内网站数量最多 3,402 个，其次是位于菲律宾和美国的 IP 地址，分别控制我国境内 3,098 个和 2,271 个网站。此外，攻击源、攻击目标为 IPv6 地址的网站后门事件有 486 起，共涉及攻击源 IPv6 地址 114 个、被攻击的 IPv6 地址解析网站域名累计 78 个。

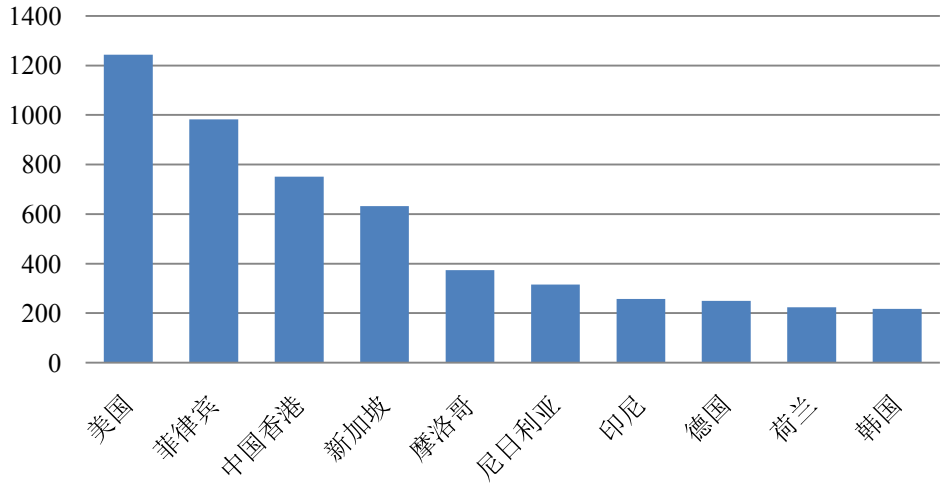

图 9 境外向我国境内网站植入后门 IP 地址所属国家或地区 TOP10

（三）网页篡改

我国境内遭篡改的网站有近 3.4 万个，其中被篡改的政府网站有 177 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 73.5%、5.4%和 1.8%，如图 10 所示。

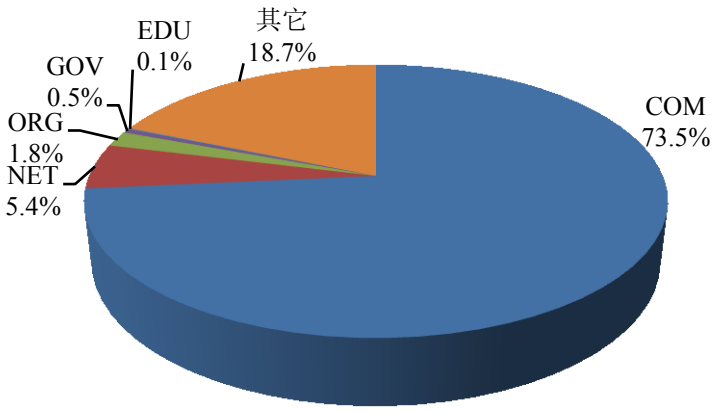

图 10 境内被篡改网站按顶级域名分布

五、云平台安全

发生在我国云平台上的各类网络安全事件数量占比仍然较高，其中云平台上遭受大流量 DDoS 攻击的事件数量占境内

目标遭受大流量 DDoS 攻击事件数的 71.2%、被植入后门网站数量占境内全部被植入后门网站数量的 87.1%、被篡改网站数量占境内全部被篡改网站数量的 89.1%。同时，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攻击的事件数量占境内控制发起DDoS攻击的事件数量的 51.7%、作为攻击跳板对外植入后门链接数量占境内攻击跳板对外植入后门链接数量的 79.3%、作为木马和僵尸网络恶意程序控制端控制的 IP 地址数量占境内全部数量的65.1%、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89.5%。

六、工业控制系统安全

CNCERT 监测发现境内大量暴露在互联网的工业控制设备和系统。其中，设备类型包括可编程逻辑控制器、串口服务器等，各类型分布如图 11 所示；存在高危漏洞的系统涉及煤炭、石油、电力、城市轨道交通等重点行业，覆盖企业生产管理、企业经营管理、政府监管、工业云平台等，如图 12、图 13 所示。

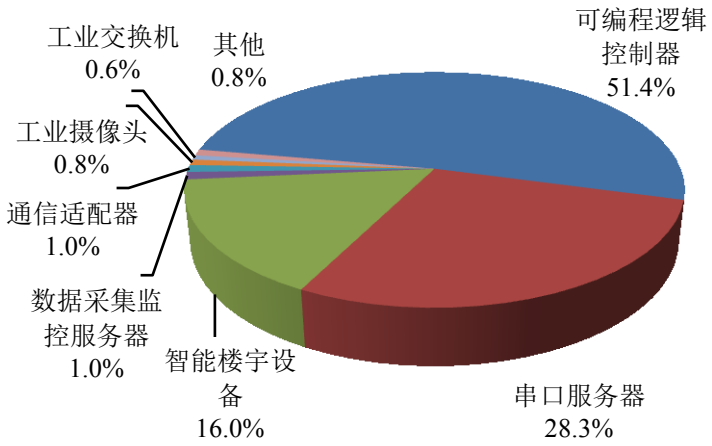

图 11 监测发现的联网工业设备的类型统计

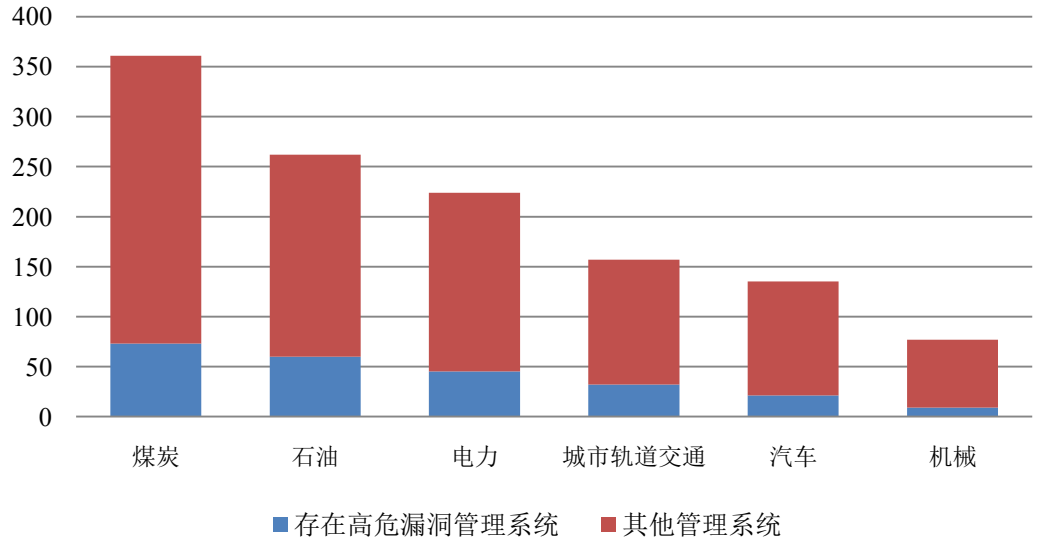

图 12 监测发现的重点行业联网监控管理系统的漏洞威胁统计

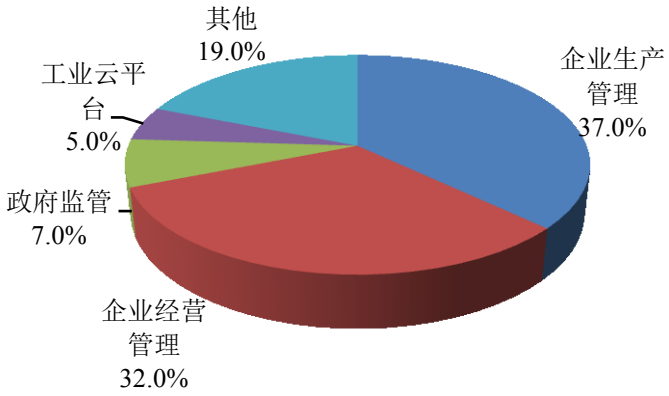

图 13 监测发现的重点行业联网监控管理系统类型统计