2020数字医疗

疫情防控期间网络安全风险研究报告

CAICT 中国信通院

中国信息通信研究院安全研究所

卫生信息安全与新技术应用专业委员会

数据保护官（DPO）社群

2020.03

版权声明

前　言

数字医疗是ICT产业融合领域的重要发展方向，网络安全是数字医疗行业健康有序发展的前提和保障。为防范和预警疫情防控期间数字医疗领域的网络安全风险，中国信息通信研究院安全研究所（以下简称：中国信通院安全所）在有关部门的指导下，联合中国卫生信息与健康医疗大数据学会卫生信息安全与新技术应用专业委员会和数据保护官（DPO）社群，共同编制了本报告。

本报告基于中国信通院安全所产业互联网安全实验室对于数字医疗领域安全状况的长期动态观测，从公共互联网安全、移动App安全、新型医疗设备和网络攻击态势等角度出发，解析了疫情防控期间医疗领域面临的网络安全风险，深度研究了网络安全风险的变化趋势，并从健全标准体系、完善平台机制、培养人员意识、建设安全能力等方面给出了工作建议，为构建和健全数字医疗网络安全体系提供思路参考。限于研究时间和编者能力，部分报告内容难免存在纰漏，不足之处恳请业界同仁批评指正。

新冠肺炎疫情仍在持续蔓延，各国均处在抗击疫情的紧要关头。防控数字医疗网络安全风险，才能更好地支撑和助力打赢疫情防控攻坚战，推动数字医疗产业融合领域的健康发展。

目 录

一、数字医疗领域网络安全总体态势

（一）数字医疗网络安全研究背景

近年来，网络安全风险急剧上升，据世界经济论坛发布的《2020年全球风险报告》统计，数据欺诈或窃取、网络攻击分别排在全球十大风险的第六位和第七位，网络安全形势极为严峻。健康医疗行业是关系国计民生的重点领域，其网络安全风险需要持续关注和研究。

2020年伊始，新冠肺炎疫情席卷全球，广大医疗机构和医务工作者奋战在抗击疫情一线。然而不法分子却假借疫情之名，开展网络攻击和网络欺诈，对疫情防控相关工作造成极其恶劣影响。

随着健康医疗产业与ICT领域的融合发展，各类新型医疗设备逐渐应用普及，并成为智慧医疗、智慧健康的重要组成部分。其在提升医疗效率、辅助医生工作的同时，也增加了网络安全防护、隐私数据管理的难度，一旦这些医疗设备发生网络安全相关问题，可能造成灾难性后果。

中国信通院安全所持续观测健康医疗行业网络安全风险，在2019年的观测报告中指出，以勒索病毒为代表的僵木蠕等恶意程序、安全隐患带来的大数据泄露和网站篡改是健康医疗行业的三大风险。随着时间推移和新冠肺炎疫情的暴发，健康医疗行业网络安全风险呈现动态变化特点，本报告

将对疫情期间的医疗网络安全风险及动态变化趋势进行重点分析和研究。

（二）数字医疗网络安全研究范围

数字医疗网络安全是攻击方与防御方的动态博弈，本报告从数字医疗行业外部攻击者视角出发，观测评估了疫情期间健康医疗行业公共互联网领域以及移动App方面的网络安全风险，分析了疫情影响下新型医疗设备应用趋势和风险，总结了疫情期间针对医疗行业的网络攻击模式，形成疫情期间整体攻击者视角数字医疗安全态势分析报告。

1、健康医疗公共互联网安全的观测范围

在公共互联网安全观测上，报告团队共观测了健康医疗领域15,948家相关单位。观测对象按职能划分，覆盖疾病预防控制中心549家，卫生监督所332家，卫生健康委员会432家，医学会170家，公立医院4,531家，私立医院9,933家。各类职能机构占比情况如图1所示。据国家卫生健康委员会官方网站统计数据显示，截止2019年11月，我国共有公立医院11,891家，私立医院2,2081家，本次观测公立医院和私立医院的覆盖度分别达到38.10%和44.98%。

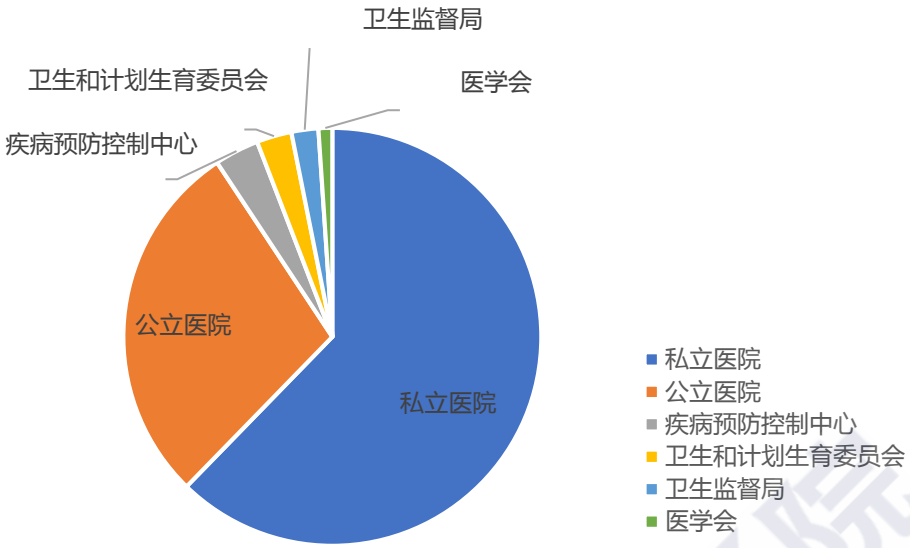

图 1 观测对象职能分布

观测范围从地域上覆盖了全国除港、澳、台以外所有的31个省、自治区和直辖市，其中山东、四川、广东、江苏、河南单位分布较多，观测单位地域分布情况如图2所示。

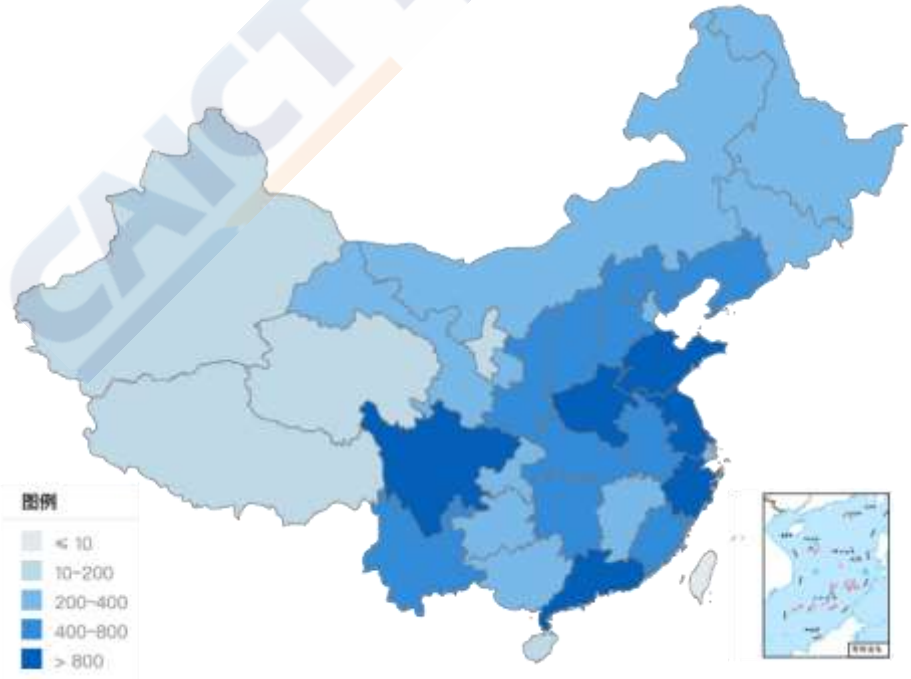

图 2 观测对象地域分布

2、健康医疗移动App安全的观测范围

在App安全观测上，为了更好评估疫情期间健康医疗App安全情况，报告团队在2020年2月份从265个安卓应用市场共收录了21,846款健康医疗类App作为观测对象。

从观测对象的地域分布来看，有20,900款App能明确归属省份，全国34个省级行政区均覆盖在内，平均每个省级行政区生成健康医疗行业App约614.7款。健康医疗行业App生成地域分布不均，北京、广东两个地域的健康医疗App最为集中，分布情况如图3所示。

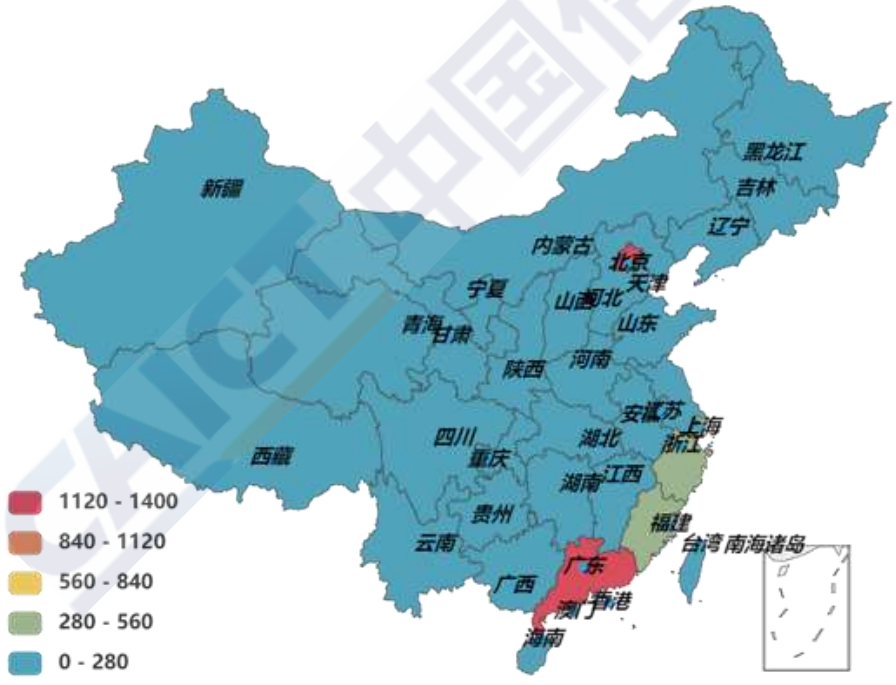

图 3 健康医疗类 App 生成地域分布情况

从应用市场来看，29.27%的健康医疗类App集中在应用宝、豌豆荚、百度手机助手等排名前十的应用市场。其中应用宝收录健康医疗App数量最多，占观测总数的5.09%；其次

是豌豆荚，收录量占观测总数的4.26%；百度手机助手排行第三，收录量占比观测总数的3.28%。收录量Top10的应用市场如图4所示。

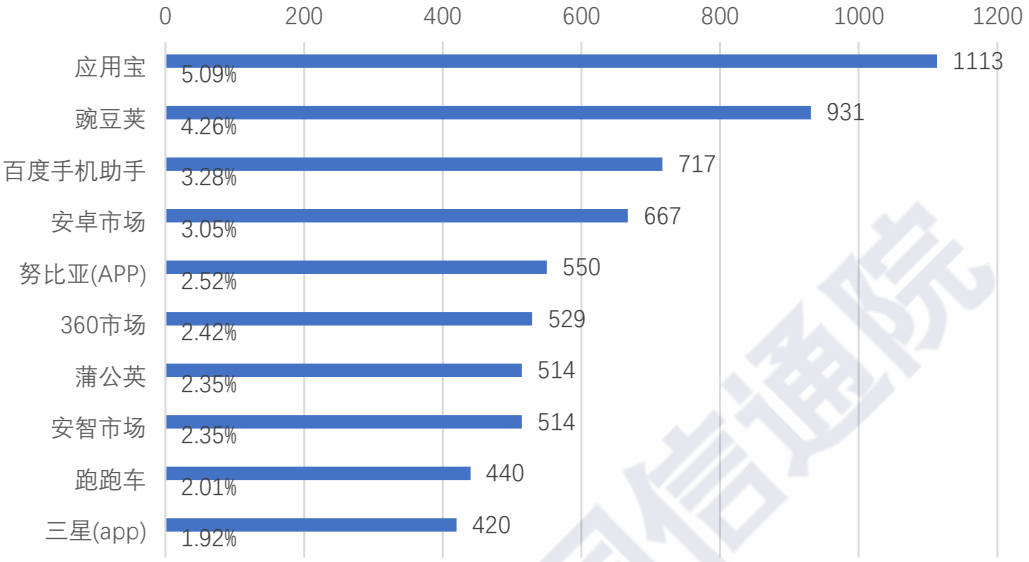

图 4 健康医疗行业 App 收录量 Top10 应用市场

（三）数字医疗安全研究结果概要

基于持续的安全观测和研究分析，本报告研究团队综合运用大数据、人工智能、威胁实时感知等技术和能力，全方位、多维度地评估了健康医疗行业的网络安全风险和动态变化趋势。从公共互联网、移动App、新型医疗设备、安全攻击四方面总结了当前健康医疗行业面临的网络安全风险。

在公共互联网安全风险变化方面，健康医疗行业网络安全风险主要表现为以下几个特点：一是数字资产暴露微降，安全隐患持续居高；二是安全漏洞修复提升，私立医院问题突出；三是僵木蠕毒风险加剧，网站篡改亟需关注；四是私立医院风险偏高，公立医院承受攻击。

在移动App安全风险方面，健康医疗行业网络安全风险归纳为以下几点：一是以App仿冒为代表的高危漏洞风险严重；二是以流氓行为为代表的恶意程序感染加剧；三是使用第三方SDK引入的安全隐患升高；四是App加固不足造成源代码暴露问题恶化。

在疫情影响下的新型医疗设备安全态势方面，主要是以下两点：一是疫情推动医疗设备行业创新发展；二是医疗设备行业安全体系亟待完善。

在网络攻击方面，疫情期间健康医疗行业主要面临以下两方面的网络攻击问题：一是疫情相关题材网络钓鱼成为主要攻击手段；二是医疗服务认证暴力破解攻击态势持续严峻。

二、疫情期间医疗公网安全风险趋势研究

（一）数字资产暴露微降，安全隐患持续居高

脆弱性指系统采取的安全策略存在不足和缺陷，存在可能被攻击者利用实施攻击的薄弱环节。本报告团队基于观测结果分析发现，健康医疗行业易被利用实施攻击的脆弱性主要集中在三个方面：**敏感服务暴露在公共互联网（39.28%）、存在公开漏洞的低版本服务（44.39%）、可被利用的高危端口开放（49.46%）。**

从安全隐患动态变化角度来看，健康医疗行业相关机构网络资产三大脆弱性问题在2月份观测中均有轻微缓解，如图5所示。但不可忽视的是，在2月份观测的单位中，存在脆弱性的单位高达10,013家，占观测单位的62.79%，健康医疗行业网络资产脆弱性问题仍然居高不下。

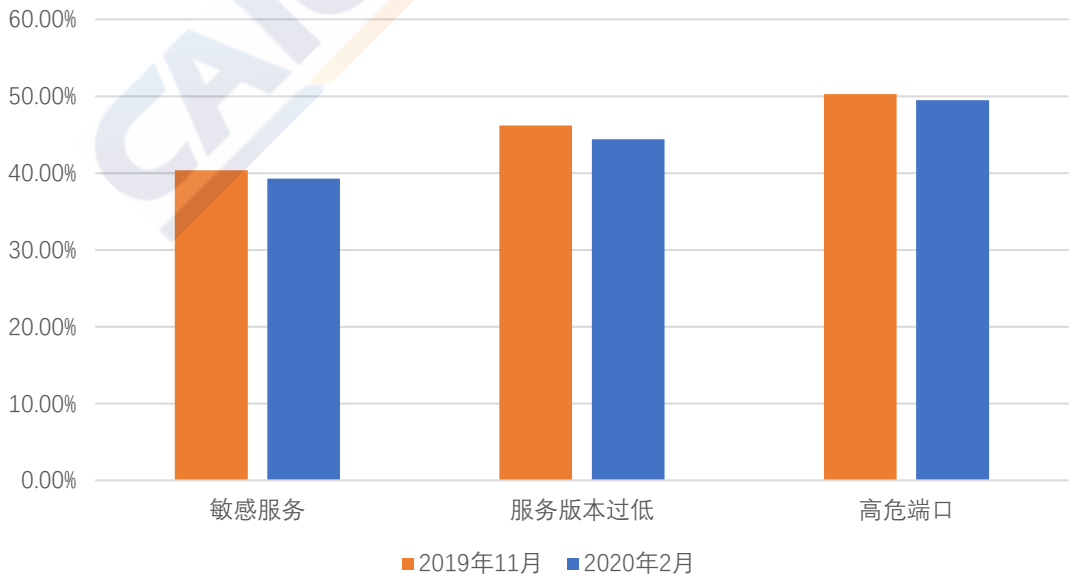

图 5 存在三大脆弱性单位占比变化情况

数据是健康医疗行业的核心资产，也是不法分子最为关注的攻击目标之一。医疗数据服务一旦在公共互联网被黑客发现，可能招致较多的网络安全攻击，进而导致数据泄漏，造成严重安全后果。在本次观测中，数据库服务、文件服务暴露在公共互联网的医疗单位占比分别达到29.8%和28.88%，共涉及2.1万项数据资产，这些暴露的数据服务给医疗行业数据安全带来巨大的安全风险。从数据服务暴露数量的省份分布情况来看，山东、广东、四川、江苏等省份暴露的数据服务数量最多，需要相应省份提升数据服务的防护水平。具体分布如图6所示。

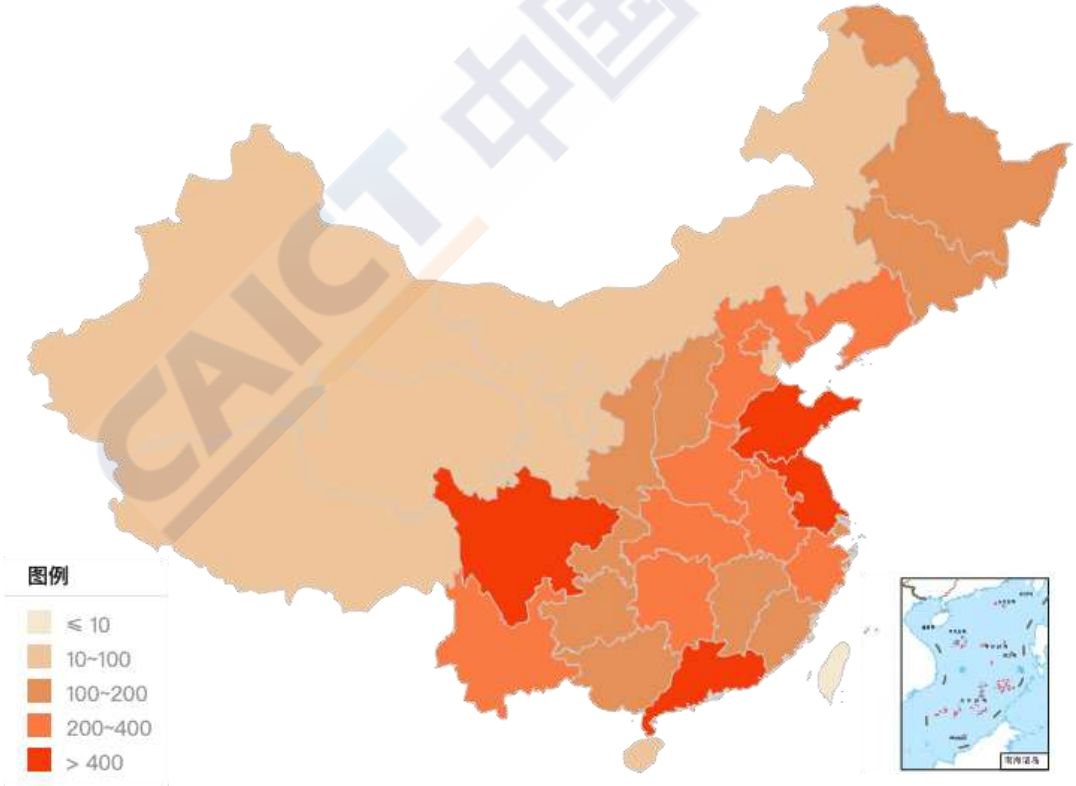

图 6 各省份数据服务暴露数量分布

应用服务组件版本的及时升级是安全防护的重要手段

之一，对于已有公开漏洞的组件版本，应及时升级更新，以避免相关安全风险。本次观测中发现，有7,080家单位使用存在公开漏洞的低版本组件服务，占全部观测对象的44.39%。具体低版本组件涉及的单位数量如图7所示。相比去年的观测结果，OpenSSH、MySQL、Apache、Nginx涉及的单位数量均有不同程度增加，其中OpenSSH增幅达到120%，可见相关安全隐患并未得到医疗单位充分重视，风险形势极为严峻。

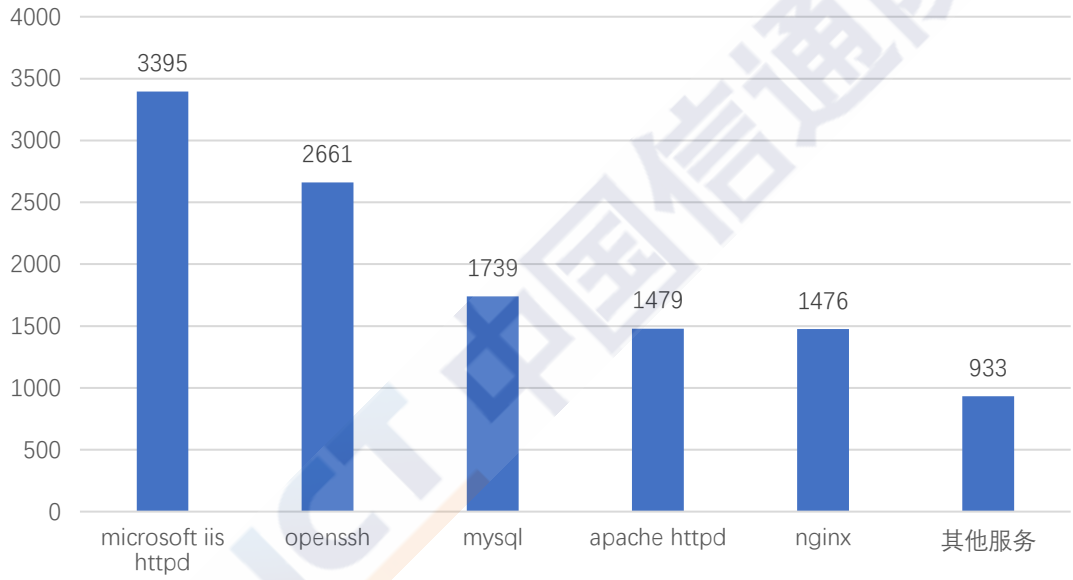

图 7 本次观测涉及较多单位的低版本服务

端口如同是服务的钥匙，一旦存在可被利用的高危漏洞，就有可能导致服务被利用，造成敏感数据窃取、服务器命令任意执行、服务器权限非法获取等严重后果。本次观测到高危端口Top10分布如图8所示。我们可以看到，开放MySQL端口3306的机构数量最多，随后是SSH端口22、Windows远程桌面端口3389和网络打印端口9100。值得注意的是，受此次新冠肺炎疫情影响，远程办公、远程运维等活动增加，开放远

程登录端口22、3389的单位数相比2019年7月增加31.76%和34.95%，这两个端口的漏洞问题需要重点关注。

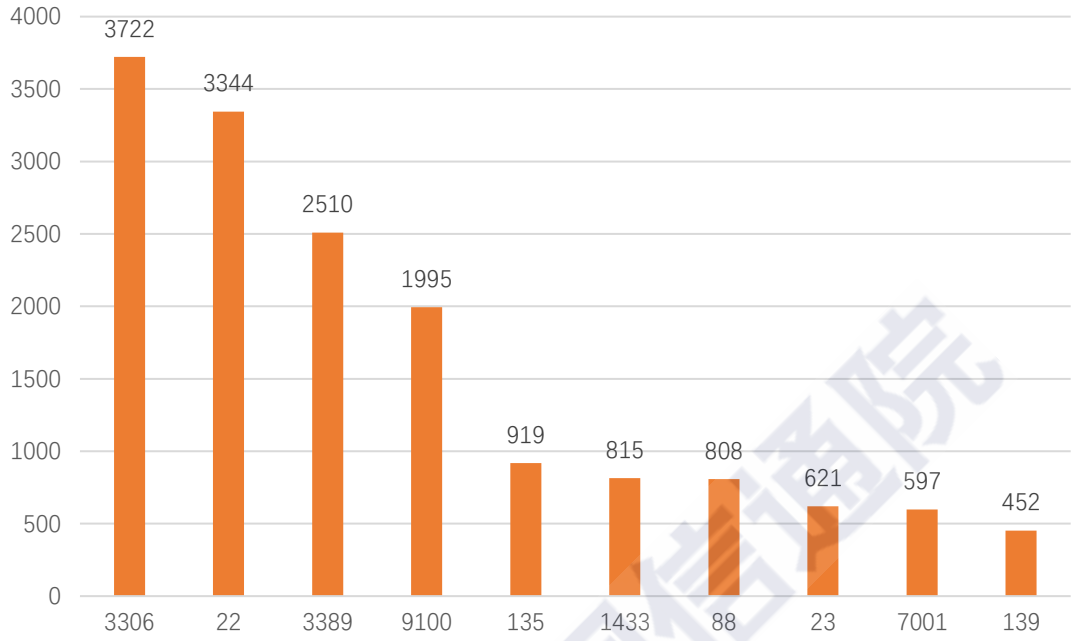

图 8 本次观测中涉及单位最多的 10 个端口

（二）安全漏洞修复提升，私立医院问题突出

研究团队针对健康医疗行业观测发现的问题进行了渗透测试，共发现330个安全漏洞，涉及251家医疗单位，占全部观测对象的1.57%，漏洞类型及分布情况如图9所示。对比2019年7月的观测结果，高危漏洞问题有较大幅度下降，主要原因来源于远程桌面远程执行代码漏洞（CVE-2019-0708）的修复，存在该漏洞的单位由2019年的1,021家下降到当前的33家。同时，弱密码问题也得到了缓解，由411家下降到了48家。Apache Struts2相关漏洞呈上升态势，建议关注该服务的相关补丁信息，及时修复漏洞。

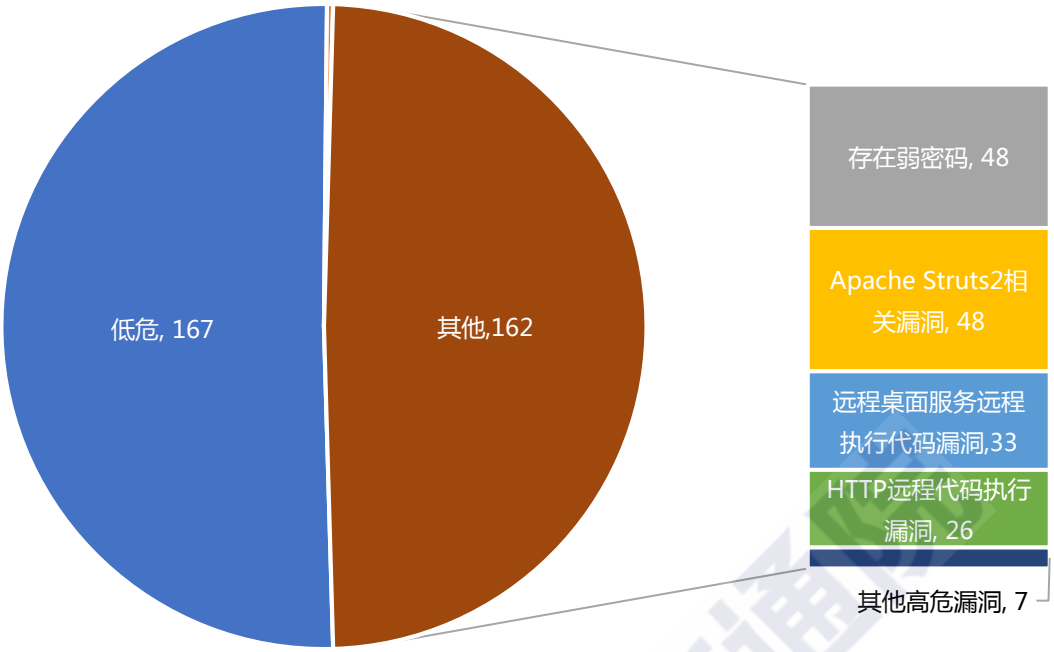

图 9 观测对象渗透测试漏洞情况

从各省存在安全漏洞单位占比情况来看，排名前四的省份分别是浙江、北京、广东、江苏，具体数据如表1所示。

表 1 存在安全漏洞单位占比排名 Top4 的省份

省份	存在漏洞单位数量	存在漏洞单位占比
浙江省	22	2.50%
北京市	19	2.38%
广东省	24	2.11%
江苏省	21	2.06%

研究团队重点关注了漏洞数量Top5的医疗机构，具体漏洞情况如表2所示。其中有1家疾病预防控制中心，该中心有19个同一类型的低危漏洞，即网站测试环境搭建使用的PHPinfo()未及时删除，暴露出网站建设人员安全意识不足的

问题。有4家私立医院，每家医院均扫描出不同类型的高危漏洞，一定程度上反应出私立医院网络安全漏洞防护相对落后。

表 2 漏洞数量 Top5 医疗机构

序号	机构	高危漏洞	中危漏洞	低危漏洞	总漏洞
1	新疆维吾尔族自治区某疾病预防控制中心	0	0	19	19
2	江苏省某私立医院	10	0	0	10
3	江苏省某私立医院	8	0	0	8
4	四川省某私立医院	8	0	0	8
5	上海市某私立医院	8	0	0	8

（三）僵木蠕毒风险加剧，网站篡改亟需关注

不法分子在攻破医疗机构服务后，往往通过植入木马病毒等恶意程序、篡改网站内容等方式实现其远程控制、数据窃取、挖矿或导流等目的。因此，观测扫描健康医疗行业机构被植入恶意程序和网站篡改等相关情况，是评估健康医疗行业遭受网络攻击情况最为直观的手段。

为了便于分析评估疫情期间健康医疗行业遭受网络攻击的变化情况，研究团队对比了2019年11月、2020年1月、2020年2月的观测数据，如图10所示。疫情暴发后，流氓或广告软件、与恶意主机通信、挖矿软件、漏洞利用等大部分恶意软件感染单位数量均呈现上升趋势，仅勒索软件微降。可

见疫情期间，健康医疗行业面临更为严峻的网络安全态势，僵尸、木马、病毒等恶意程序感染风险更高，亟需提高安全防护意识和建立安全防护手段。

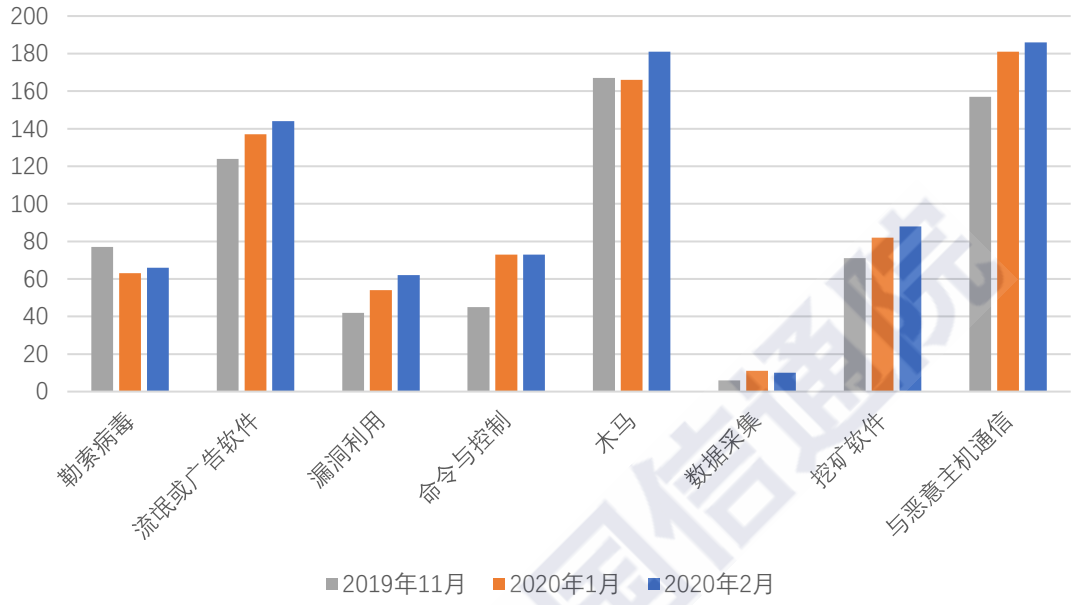

图 10 各类恶意程序数量情况

表3列举了受到恶意程序感染最为严重的10家医疗机构，其中8家为公立医院，2家为私立医院。这些医院感染的恶意程序总量达到907个，占到全部恶意程序样本总量的26.28%，相关医院亟需提升恶意程序监测和防护能力。

表 3 感染恶意程序数量 Top10 医院

序号	恶意程序数量	省份	机构类型
1	115	江西省	公立医院
2	115	新疆维吾尔族自治区	私立医院
3	109	贵州省	公立医院
4	95	江苏省	公立医院

序号	恶意程序数量	省份	机构类型
5	88	安徽省	公立医院
6	87	广西壮族自治区	公立医院
7	83	浙江省	公立医院
8	79	重庆市	私立医院
9	73	广东省	公立医院
10	63	浙江省	公立医院

根据网站篡改效果，网站篡改可分为显式篡改和隐式篡改两种。显式篡改主要用于帮助攻击者声明自己的主张，因此篡改内容可见，如果改为非法信息，影响极其恶劣。隐式篡改的内容不可见，一般通过植入色情、博彩、诈骗等非法信息，帮助攻击者谋取非法经济利益。本次观测中发现被篡改的网站共涉及171家单位，其中篡改为博彩的网站涉及单位157个，篡改为色情的网站涉及单位18个。

从网站篡改的攻击趋势来看，2020年2月网站篡改类攻击相比2019年11月明显增长，增长幅度达到44.92%，且在各类机构增长趋势基本一致，如图11所示。

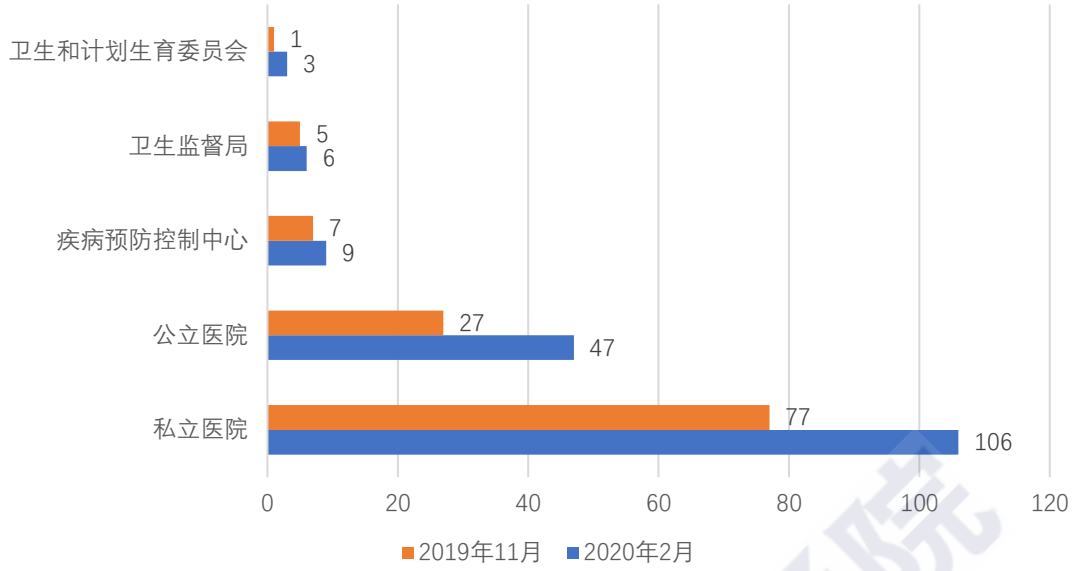

图 11 各类机构网站篡改变化情况

（四）私立医院风险偏高，公立医院承受攻击

从数字资产三大脆弱性方面对比公立医院与私立医院可以看到，虽然公立医院和私立医院均存在较高比例的网络安全隐患，但公立医院在三大脆弱性防护方面要强于私立医院，一定程度可以反映出公立医院的安全防护意识相对私立医院更强，具体数据如图12所示。

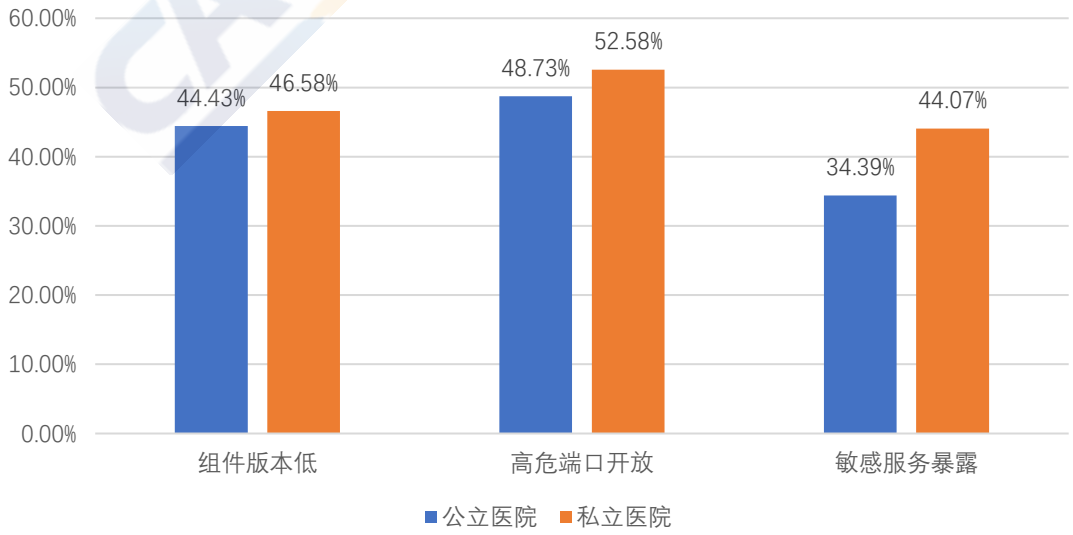

图 12 存在脆弱性的单位占比

在安全漏洞层面，存在高危和低危安全漏洞的私立医院占比都超过公立医院。具体数据如图13所示。

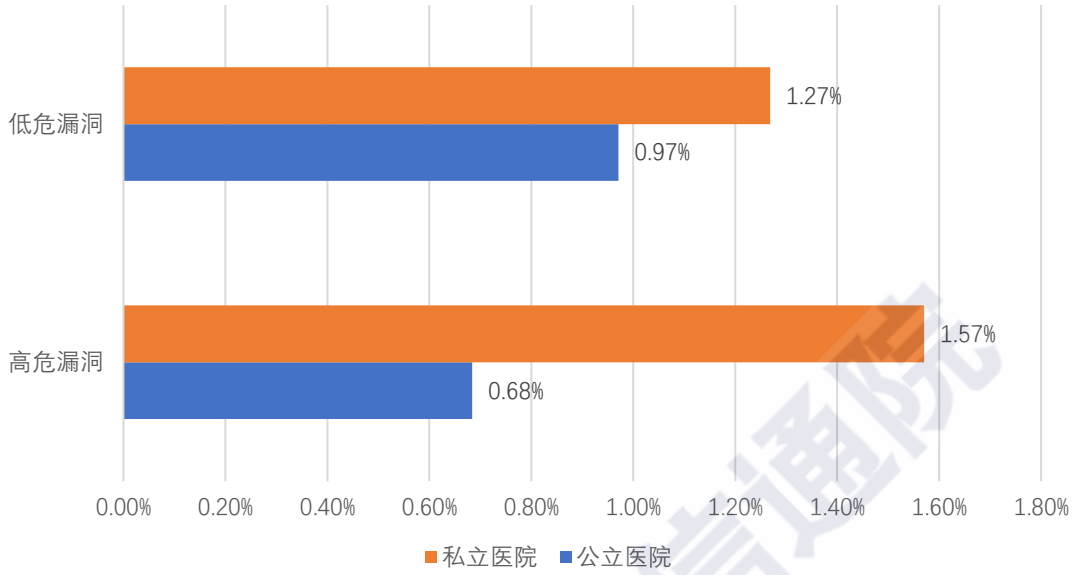

表 13 存在安全漏洞的单位占比

在恶意程序感染方面，公立医院受到恶意程序感染的医院数量和比例都超过私立医院，且随着新冠肺炎疫情的暴发，受恶意程序感染的单位数量呈现上升趋势，而私立医院则没有表现出类似特点，具体数据如图14所示。

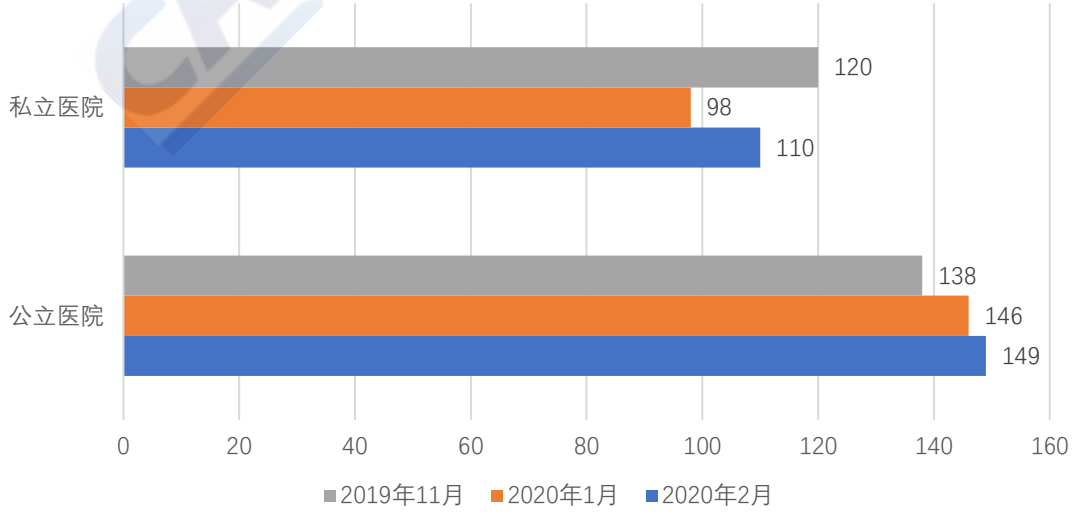

图 14 不同类型机构受到恶意程序感染情况

综合以上分析可知，在网络安全风险防护方面，公立医院的安全意识和手段要强于私立医院，私立医院相较面临着更大的网络安全风险。然而，从实际攻击结果方面，公立医院被感染和植入的恶意程序更多，且随着疫情暴发呈现增长趋势，可以推断公立医院承受更多的安全攻击压力。

三、疫情期间移动医疗 App 安全风险评估

（一）以 App 仿冒为代表的高危漏洞风险严重

报告团队对21,846款健康医疗行业App进行漏洞扫描，共计检测出346,974条漏洞记录，涉及61种漏洞类型，其中高危漏洞有23种。健康医疗行业App中，84.15%存在不同程度的安全漏洞，平均每款App存在18.88个漏洞，81.24%的App存在高危漏洞，虽然存在高危漏洞App相比2019年的88.83%有所下降，但健康医疗App的高危漏洞风险仍然非常严重。不同漏洞数量对应的App分布情况如图15所示。

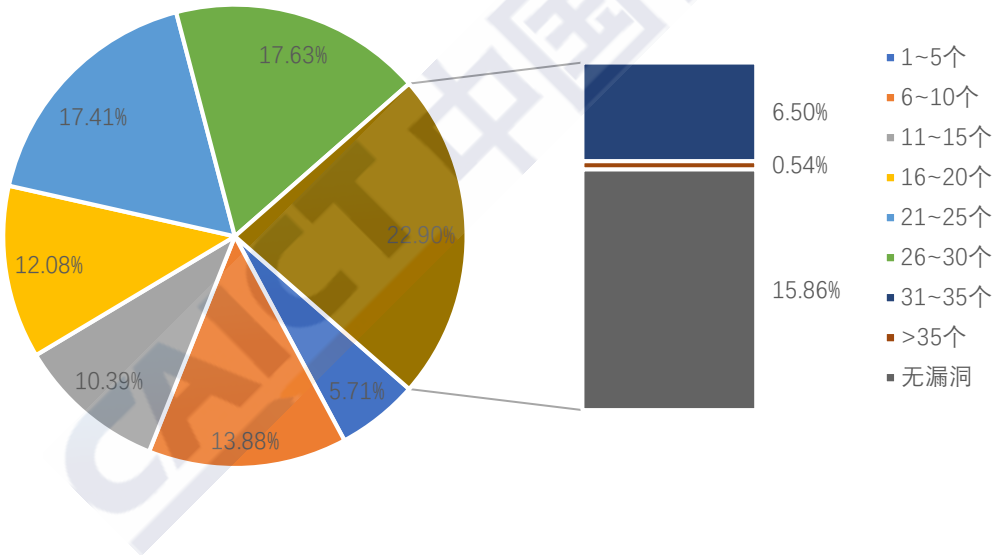

图 15 不同漏洞数量对应的 App 分布情况

从高危漏洞类型来看，存在Janus漏洞的App数量最多，占监测总数的66.08%；其次是Java代码加壳检测，占监测总数的53.89%；WebView远程代码执行漏洞排行第三，52.24%的App存在此漏洞。攻击者可利用这些漏洞进行App仿冒、植

入恶意程序、窃取用户敏感信息、攻击服务等，对App安全具有严重威胁。高危安全漏洞Top10如图16所示。

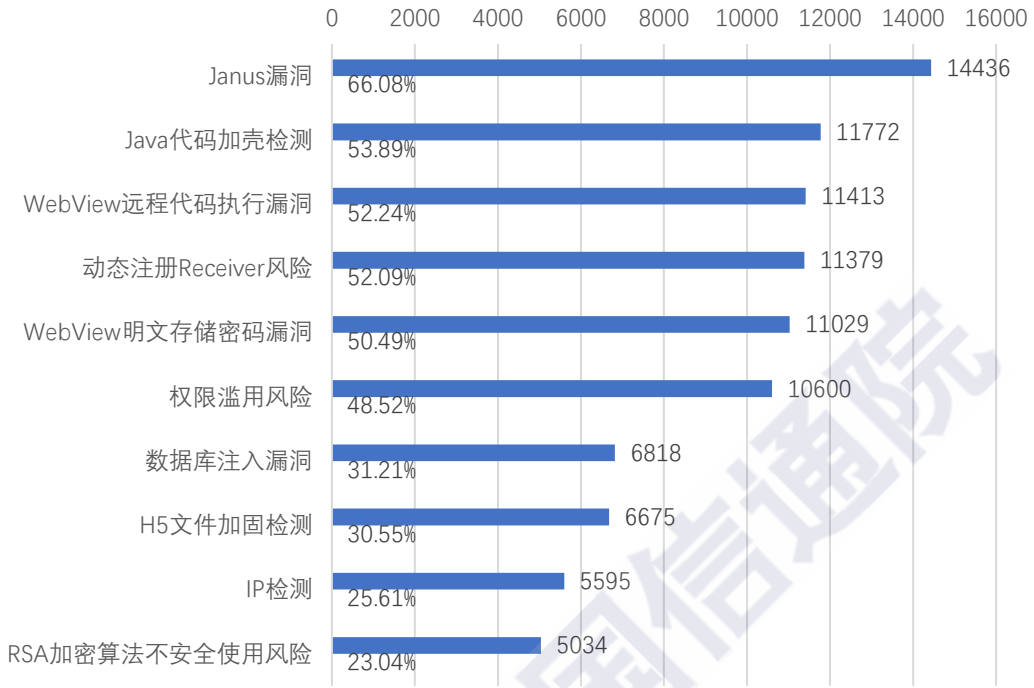

图 16 高危漏洞类型 Top10 分布

（二）以流氓行为为代表的恶意程序感染加剧

在恶意程序方面，共有806款健康医疗App被检测出含有恶意程序，感染恶意程序App占比达到3.69%，而2019年健康医疗App恶意程序感染率仅为0.86%，可见健康医疗App恶意程序感染风险加剧，需要重点关注。从恶意程序类型来看，64.05%的App受到具有流氓行为的恶意程序感染，这类恶意程序会在用户未授权的情况下，任意弹出广告窗口，影响用户体验的同时，可能因误触点击导致隐私安全风险；16.01%的App受到具有资费消耗行为的恶意程序感染，这类恶意程序会在用户不知情或未授权情况下，通过频繁连接网络等方

式导致用户资费损失，具有资费消耗属性。存在不同恶意程序类型的应用占比如图17所示（一款App可能存在多种恶意程序）。

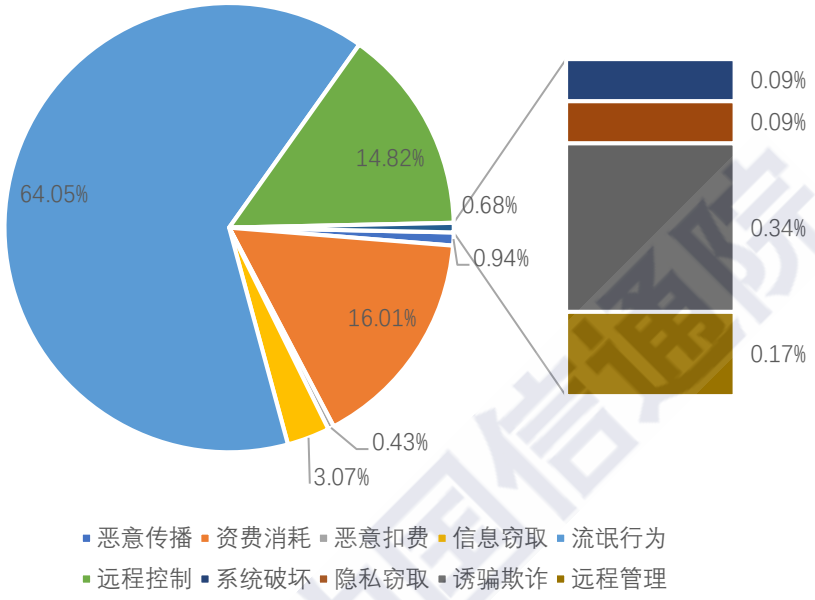

图 17 App 恶意程序分布情况

（三）使用第三方 SDK 引入的安全隐患升高

SDK是Software Development Kit的缩写，即“软件开发工具包”，它是辅助开发某一类应用软件的相关文档、范例和工具的集合。随着移动互联网的快速迭代发展，越来越多的服务提供商选择将其服务封装成SDK供开发者使用。而开发者为了提升效率、降低成本，往往会在开发过程中嵌入第三方SDK。但是，第三方SDK常存在安全漏洞、恶意程序、隐蔽收集个人信息等安全问题，进而给嵌入SDK的App带来相应的安全隐患。本次检测发现，共有9,636款健康医疗行业App嵌入了第三方SDK，占检测总数的44.11%，平均每款APP嵌

入2.37个，嵌入5个及以上SDK的App占比9.88%。对比来看，2019年健康医疗行业App被嵌入第三方SDK的比例仅有25.58%，可见在健康医疗行业App中第三方SDK使用更为普遍，SDK应用带来的安全隐患也在持续升高。

（四）App 加固不足造成源代码暴露问题恶化

基于Java编写的安卓App容易被破解暴露App源代码，进而带来App盗版、二次打包、注入等安全问题。“安全加固”是维护App安全的重要防护手段，它能够有效阻止对App的反汇编分析。经过安全加固的App，不仅其系统稳定性得到提升，还拥有能力规避一定程度的安全风险。本次检测发现，健康医疗行业App加固比例降低至18.04%（2019年其加固比例为24.83%），有超过80%的App未进行过安全加固，安卓App源代码暴露风险进一步恶化。

四、疫情期间新型医疗设备应用风险分析

（一）疫情推动医疗设备行业创新发展

长久以来，医药产业中对医疗设备重视程度低于药品，而在此次新冠肺炎疫情中可以发现，能够快速诊断的医疗设备和试剂十分重要。然而医疗设备产品上市前需要经过注册检验、临床评价、技术审评等多个环节，门槛要求很高。在疫情防控过程中，在政府政策的推动下，行业诸多科研人才投入到了攻关创新型医疗设备中，各类结合AI技术、机器人技术的新型医疗设备逐步应用推广。例如搭载AI的专用CT机设备，能够快速识别新冠肺炎影像，大幅度降低医生阅片工作量；各类提供消毒、送餐、配药、测温、问诊、护理、陪伴、运输、超声等服务的机器人医疗设备冲上防御一线，在疫情防控工作中扮演了重要角色；基于5G技术的远程诊疗视频设备、超声设备、手术设备等，支撑了疫情期间的远程医疗协同、会诊、手术的高效应用。新型医疗设备在新冠肺炎疫情的推动下快速走向市场和实践。

与此同时，此次疫情也刺激了医疗设备市场的快速发展，据亿邦动力统计，自2020年1月1日至2月7日，全国超过3,000家企业经营范围新增了“医疗器械”业务。

（二）医疗设备行业安全体系亟待完善

在各类新型医疗设备应用推广的同时，我们需要警惕新

型医疗设备应用带来的网络安全风险。由于医疗设备的特殊性，一旦发生网络安全问题，可能直接危及患者的生命健康，造成极其严重的后果。美国食品药品管理局（Food and Drug Administration，简称FDA）在2019年1月至2020年3月间公布了23起医疗设备安全事故，其中5起都是由网络安全问题引起的，可见医疗设备网络安全风险形势不容乐观。

当前，我国针对医疗设备上市后的监管主要是通过不良事件报告及召回的方式，但由于医疗设备生产企业对不良事件和其他安全问题上报不及时，而导致使用单位或使用者面临巨大损失的情况时有发生。据国家药品监督管理局在2019年10月发布的《国家医疗器械不良事件监测年度报告（2018年）》显示，全国医疗器械不良事件监测信息系统在2018年接收到可疑医疗器械不良事件监测报告达到40余万份。随着各类新型医疗设备的落地应用，医疗设备网络安全将面临巨大的挑战。我国针对医疗设备的网络安全监管仍处于建设期，各类医疗设备网络安全监管标准体系和机制手段需要进一步健全和完善。

五、疫情期间医疗网络安全攻击特征总结

（一）疫情相关题材网络钓鱼成为主要攻击手段

借助热点事件传播病毒和开展网络攻击一直是黑客的惯用攻击手段。此次新冠肺炎疫情暴发后，利用新冠肺炎相关题材的网络钓鱼攻击事件频发，成为疫情期间最为主要的网络攻击手段。

研究团队基于观测数据发现，此次借助新冠肺炎疫情开展网络钓鱼的病毒木马恶意程序以文件夹病毒、蠕虫病毒、后门远控木马、后门程序木马等类型为主，并冠以“武汉肺炎”、“新型肺炎”、“冠状病毒”、“疫情动态”、“口罩厂家名单”等涉及疫情的关键字。黑产团队通过修改病毒样本名称，伪装后诱导受害者下载运行，实现窃取数据、控制用户设备等目的。以此手段开展网络钓鱼攻击的组织涉及APT组织、黑客以及黑产团伙，受到此类钓鱼攻击的地域涉及中国、美国、日本等多个国家。

研究团队整理此类网络钓鱼攻击的6个典型样本，分别为“新型冠状病毒配方.com”、“open新型冠状病毒资料.exe”、“5名医务人员感染新型冠状病毒!!.com”、“新型冠状病毒培训班.exe”、“疫情杂物.exe”、“疫情重要事项报告.exe”，可用于全网布控和防护。

（二）医疗服务认证暴力破解攻击态势持续严峻

春节假期是企业“封网”的休息时期，企业安全策略更新时效性相比平时较差，本身容易吸引黑客在此时期发动攻击。新冠肺炎疫情暴发后，为避免人员聚集产生的交叉传染风险，大量企事业单位延迟复工或远程办公。企业为了员工远程办公便利，往往对外开放远程服务，直通敏感信息系统甚至办公内网。在这种情况下，认证暴力破解成为黑客最常使用的手法。在1月31日（正月初七，即往年开工首日），黑客对医疗行业的暴力破解攻击达到了单日80万次的高峰。Windows生态中的远程桌面服务RDP和数据库服务SQL Server成为受到攻击的重灾区，攻击数据如图18所示。

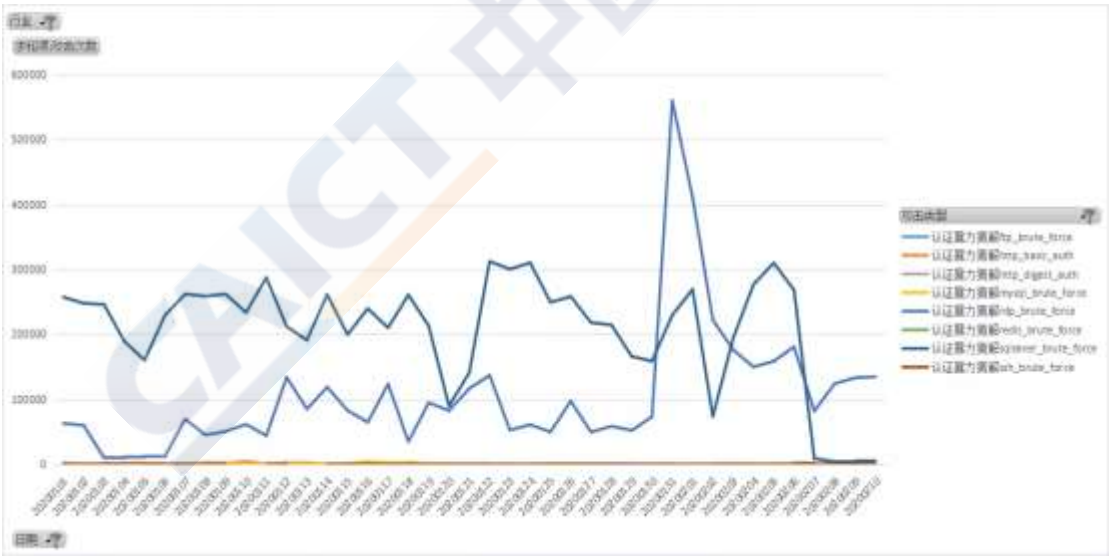

图 18 医疗行业被暴力破解攻击态势

从攻击源分布上看，针对腾讯云上医疗行业客户的认证暴力破解攻击超过70%来自境外125个国家。由于美国区域机房管控趋严，使得美国成为攻击源的“冷门片区”，而来自印

度、俄罗斯的国家的攻击跃居前列。与此对应的是，传统Web攻击源绝大部分来自境内，春节期间攻势迅速下降达到了低谷。

六、疫情期间网络安全工作思路建议

（一）强化安全标准，规范行业发展

健康医疗行业网络安全标准化工作是健康医疗领域网络安全保障体系建设的重要组成部分,在推动健康医疗领域网络安全治理体系变革方面发挥着不可替代的作用。安全标准体系的制定、完善和落地，有助于规范和推动医疗信息化、医疗App及医疗设备等全医疗领域数字化的安全建设。随着物联网、5G等新技术在数字医疗领域的深度应用，新型医疗设备和医疗应用不断涌现，亟需健全完善的健康医疗行业网络安全标准化体系建设。应充分利用ICT领域新技术安全应用实践经验，支撑和构建新型医疗设备和医疗应用等领域的安全标准体系，推动数字医疗与ICT融合领域安全发展。

（二）持续动态监测，建立反馈闭环

网络安全风险具有长期性和动态变化的特点，且不同行业的网络安全风险特点不同。因此，建立健康医疗行业维度的网络安全风险观测机制和平台十分重要。与此同时，风险动态监测需要与风险反馈处置形成闭环，将监测到的安全风险尽快反馈到存在风险的医疗机构，修复相关安全漏洞或升级相关服务版本，从而有效控制和降低健康医疗行业整体的安全风险。

（三）加强安全培训，提高安全意识

相关人员网络安全意识不足是健康医疗行业面临的重大安全挑战。实际上，在安全观测中发现的数据服务暴露、组件版本过低以及高危端口开放等安全隐患，都直接或间接与人员网络安全意识不足存在关联。应推动和加强健康医疗行业从业人员网络安全相关培训，建立健全医疗机构内部网络安全管理规章制度，从医疗信息系统安全设计研发维护、医疗设备安全操作运维管理、医疗数据安全采集存储共享等多方面、全视角规范内部安全操作流程，切实提升相关人员的网络安全意识，落实网络安全责任。

（四）突出能力建设，形成长效机制

健康医疗行业相关机构应提升自身网络数据安全综合防护能力，加强在网络数据安全领域的投入，建立系统化的安全保障体系，构建安全长效机制：

- 加快推进网络安全等级保护测评工作，定位安全问题，排除安全隐患。
- 定期开展网络安全风险评估工作，评估医疗设备、医疗信息系统安全状况，发现潜在的安全风险。
- 协同国家专业安全机构，建立新型医疗设备和技术的安全融合应用机制，保障数字医疗新技术的安全发展。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：18610049972

电子邮箱：guofei@caict.ac.cn, zhangxueyang@caict.ac.cn

传真：010-62300264

网址：www.caict.ac.cn