2019
健康医疗行业网络安全观测报告

2019·07

CAICT 中国信通院 | 腾讯安全

联合出品

中国信息通信研究院安全研究所
腾讯科技（深圳）有限公司
卫生信息安全与新技术应用专业委员会
中国医院协会信息管理专业委员会

目 录

前 言

坚持以习近平新时代中国特色社会主义思想为指导，全面贯彻党的十九大会议精神，为支撑健康医疗大数据服务的安全管理，促进“互联网+医疗健康”安全发展，充分发挥健康医疗大数据作为国家重要基础性战略资源的作用，根据《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》等法律法规和《健康中国行动（2019—2030 年）》《国务院促进大数据发展行动纲要》《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》《国家健康医疗大数据标准、安全和服务管理办法（试行）》等文件精神，中国信息通信研究院（以下简称：中国信通院）在有关领导部门的指导下，联合腾讯科技（深圳）有限公司（以下简称：腾讯）、卫生信息安全与新技术应用专业委员会（以下简称：专委会）和中国医院协会信息管理专业委员会（以下简称：CHIMA）等相关单位、组织，依托“产业互联网安全实验室”的平台能力，梳理健康医疗行业的观测结果，探究健康医疗行业的网络安全问题，总结形成本观测报告。

本次观测行动通过公共互联网发起，共涉及全国 31 个省市地区健康医疗行业的 15339 家相关单位。经过持续数月的观测，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、多维度地梳理了健康医疗行业的网络安全现状，并采用风险量化的方法对本次观测的结果进行评估。评估发现，健康医疗行业总体处于“较大风

险”的安全风险级别，网络安全风险的集中表现，**一是**僵木蠕等问题严峻，勒索病毒威胁严重，**二是**数据泄露事件高发，应用服务存在隐患，**三是**网站篡改手法多变，隐式植入非法信息。分析其主要原因，**一是**端口存在高危漏洞，易被僵木蠕等恶意程序利用，**二是**大量敏感服务暴露，弱口令成主要安全隐患，**三是**应用组件版本较低，网站篡改概率较高。

本报告旨在通过公共互联网的安全观测，针对健康医疗行业的互联网暴露面问题进行技术研究与分析，以威胁信息共享与安全情报挖掘为基础，通过各单位的协同联动，促进健康医疗行业的网络安全防御体系建设，支撑保障互联网医疗的安全发展。

01

健康医疗行业网络安全背景

1.1 健康医疗的政策背景

自十八大以来，党中央、国务院高度重视健康医疗大数据的创新发展，习近平总书记指出，要运用大数据促进保障和改善民生，推进“互联网+医疗”。李克强总理强调，发展和应用好健康医疗大数据，是一项重大民生工程。近年来，新兴技术与健康医疗加速融合，在健康医疗大数据蓬勃发展的过程中，也面临一些新的挑战，需要及时加以引导和规范，尤其表现在“互联网+医疗”的新形态模式。

为进一步贯彻落实习近平总书记网络强国战略思想，促进“互联网+医疗健康”安全发展，根据《中华人民共和国网络安全法》《国务院办公厅关于促进“互联网+医疗健康”发展的意见》《国家健康医疗大数据标准、安全和服务管理办法（试行）》等系列文件精神，中国信通院安全所与腾讯安全联合成立了“产业互联网安全实验室”，积极构建政产学研用深度融合的协同发展创新模式，充分发挥专业机构在健康医疗领域网络安全保障的支撑作用。同时，搭建了“产业互联网安全观测平台”，对健康医疗行业网络安全态势进行实时观测，实现健康医疗领域的网络安全威胁感知，并且为完善健康医疗领域网络安全保障体系建设、提升健康医疗领域网络安全防护能力、切实筑牢健康医疗行业网络安全屏障提供重要支撑。

1.2 网络安全的现状解读

当前全球信息化进程已进入全面渗透阶段，健康医疗行业作为关乎国计民生的重要领域，是信息时代极力突破和改善的重点。我国医疗信息化目前已步入智慧医疗建设阶段，电子病历、预约诊疗、智能导诊、电子支付等网络信息技术在健康医疗便捷普惠、医疗资源压力释放、医疗资源优化配置、数据信息开放共享等方面发挥了重要作用。与此同时，频发的医疗大数据泄露、医疗系统瘫痪等安全事件逐渐引发人们对健康医疗行业信息化的安全思考，健康医疗行业网络安全配套政策法规不完善、管理规范适用性低、技术手段薄弱等问题逐步显现，健康医疗行业网络安全形势日益严峻，亟待加强健康医疗行业网络安全监管，提升健康医疗大数据安全防护能力，保障大数据安全与医疗信息化的稳定发展。

以发展的眼光来看，网络安全是攻击方与防御方之间的动态博弈，新的攻击手段不断诞生，防御方法也不断升级。但是由于网络安全攻防双方的信息不对称，往往导致防御方难以预测攻击方将在何时、何处、以何种手段发起攻击。因此，防御方经常处于被动地位，防御升级会滞后于新的攻击。解决这个问题的根本方法在于消除信息不对称，这需要联合具备公共互联网观测能力的机构，以公共互联网安全观测和安全情报挖掘为基础，内外协同构建安全防御体系，从而构筑防护范围更为广泛的有效防御联动网络。

据此，由中国信通院牵头，腾讯安全等单位参与，对健康医疗行业的公共互联网网络安全现状进行观测。此外，联合专委会、CHIMA 等组织，采用问卷调查的方式对我国部分医院的安全建设情况进行调查，形成本报告，为健康医疗行业管理部门、医疗机构和信息安全厂商提供决策依据。

1.3 公共互联网观测结果

1、 观测范围分布情况

本次观测行动通过公共互联网发起，共涉及健康医疗行业的 15339 家相关单位。观测范围从职能划分上看，覆盖疾病预防控制中心（以下简称“疾控中心”）563 家，卫生监督所（以下简称“监督所”）333 家，卫生和计划生育委员会（以下简称“卫计委”）432 家，医学会 163 家，公立医院 4143 家，私立医院 9705 家。

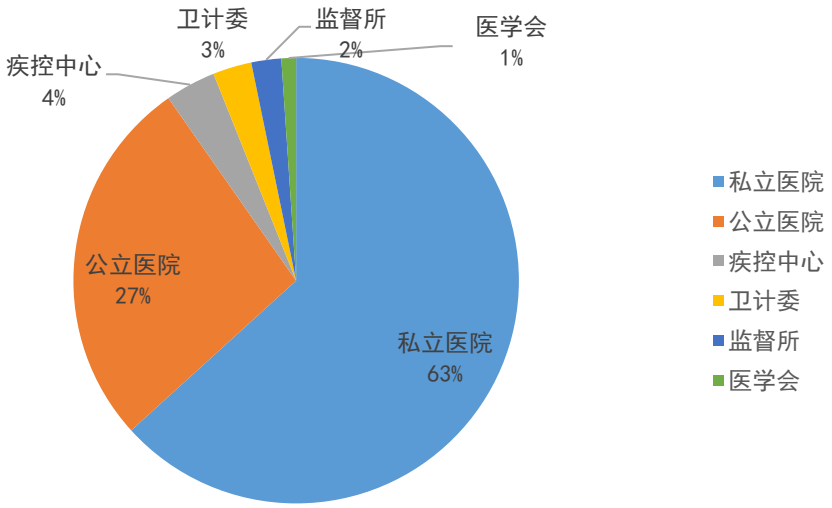

图 2.1 观测范围-以职能划分的分布图

观测范围从地域划分上看，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、河南、江苏、四川、浙江、广东属于单位分布较多的省份。

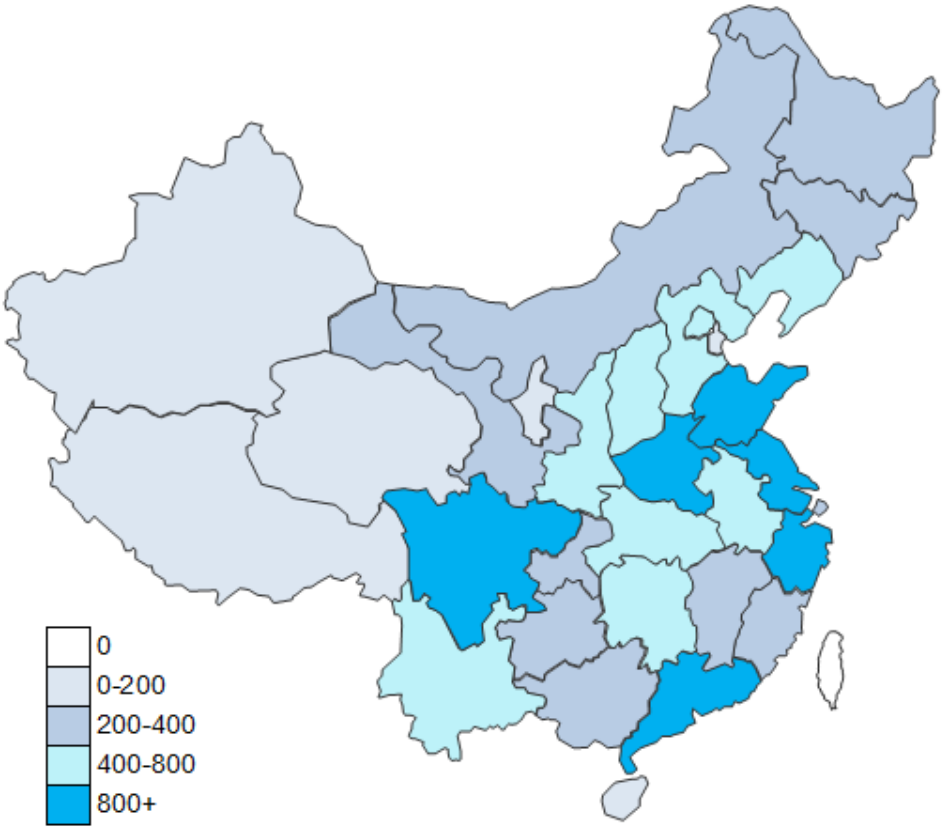

图 2.2 观测范围-以地域划分的分布图

2、观测结果评估情况

经过持续数月的观测，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、多维度地梳理了健康医疗行业的网络安全现状，并采用风险量化的方法对本次观测的结果进行评估。

（1）风险分布评估

本报告将风险分为四个级别，分别为重大风险（0-500 分）、较大风险（500-800 分）、一般风险（800-900 分）和低风险（900-1000 分）。分数越高，网络安全风险越低；分数越低，网络安全风险越高。

本次观测健康医疗行业整体评分为 788 分，总体行业处于“较大风险”的风险级别，存在多种网络安全风险以及大量可以被利用的安全隐患，防御公共互联网攻击的能力较弱。

风险级别	对应分数段	风险级别说明
重大风险	0-500 分	威胁种类多、攻击频率高，存在大量安全隐患，缺乏安全防护能力
较大风险	500-800 分	威胁种类较多、攻击频率较高，存在较多安全隐患，缺乏基础的安全防护能力
一般风险	800-900 分	威胁种类一般、攻击频率一般，存在安全隐患，具备基础的安全防护能力
低风险	900-1000 分	威胁种类较少，攻击频率较低，存在较少的安全隐患或暂未发现网络安全风险，具备较强的安全防护能力

表 2.1 网络安全风险分级

各省份风险量化的评估结果分布如下图所示。

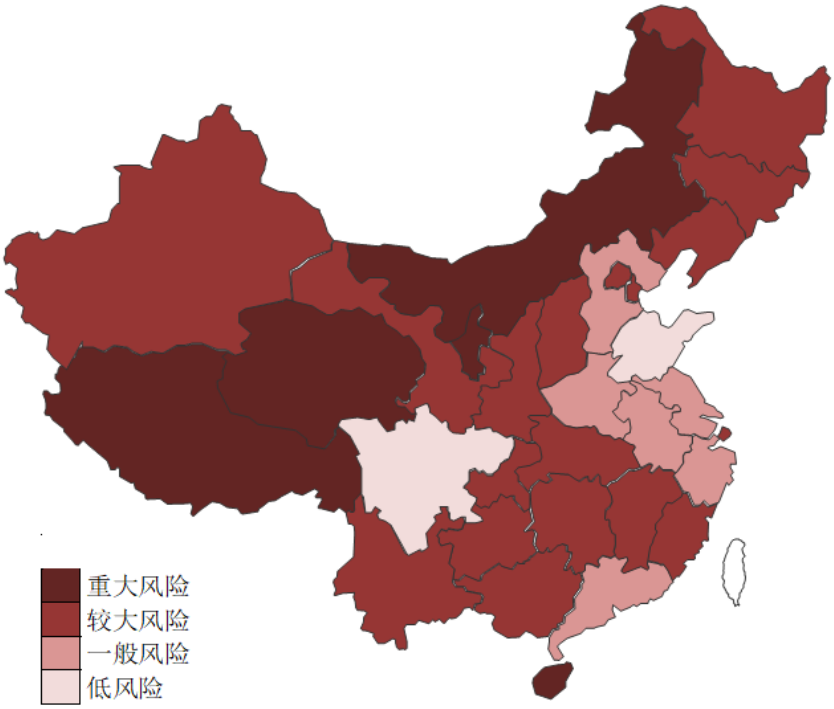

图 2.3 各省份风险评估结果分布图

- 风险级别为“低风险”的省份有：山东省和四川省；
- 风险级别为“一般风险”的省份有：浙江省、江苏省、河南省、广东省、安徽省、河北省等；
- 风险级别为“较大风险”的省份有：北京市、上海市、重庆市、天津市、福建省、山西省、甘肃省、贵州省、黑龙江省、湖北省、湖南省、江西省、吉林省、辽宁省、

陕西省、云南省、广西壮族自治区、新疆维吾尔自治区等；

- 风险级别为“重大风险”的省份有：青海省、海南省、内蒙古自治区、西藏自治区、宁夏回族自治区。

（2）风险集中表现

本次观测发现，健康医疗行业面临的网络安全风险主要集中表现在三大方面：

- **以勒索病毒为代表的僵木蠕等恶意程序风险**

在本次观测中，发现存在僵木蠕等恶意程序的单位共计 1029 家，其中受勒索病毒影响的单位共计 136 家。这些恶意程序可导致大范围的网络欺诈、信息泄露和医疗信息系统瘫痪等破坏性后果。

- **安全隐患带来的大数据泄露风险**

本次观测发现，有 6446 家单位的应用服务（如数据库服务、FTP 服务、打印机服务等）端口暴露在公共互联网，其中 375 家单位的应用服务使用了极简易的密码，攻击者可通过公共互联网轻易获取到这些服务的控制权，可能引发批量应用服务被恶意控制、大量健康医疗数据泄露的安全事件。

- **网站篡改风险**

本次观测发现，有 4546 家单位网站存在安全隐患，其中 261 家单位的网站已发现被恶意篡改的情况。如果在国家重大活动保障的政治任务期间，医院官方网站遭遇了恶意篡改、发布“黄、赌、毒”等非法信息，将造成严重的社会影响。

02

公共互联网的安全风险研究

2.1 僵木蠕等问题严峻，勒索病毒威胁严重

本次观测中发现的僵木蠕等恶意程序从地域分布上来看覆盖了全国各个省份。鉴于各省信息化程度不同导致涉及公共互联网业务的单位数目差异较大，因此对各省单位存在僵木蠕等恶意程序的占比情况进行了对比分析，发现青海省、广西省、贵州省、湖北省占比最高。

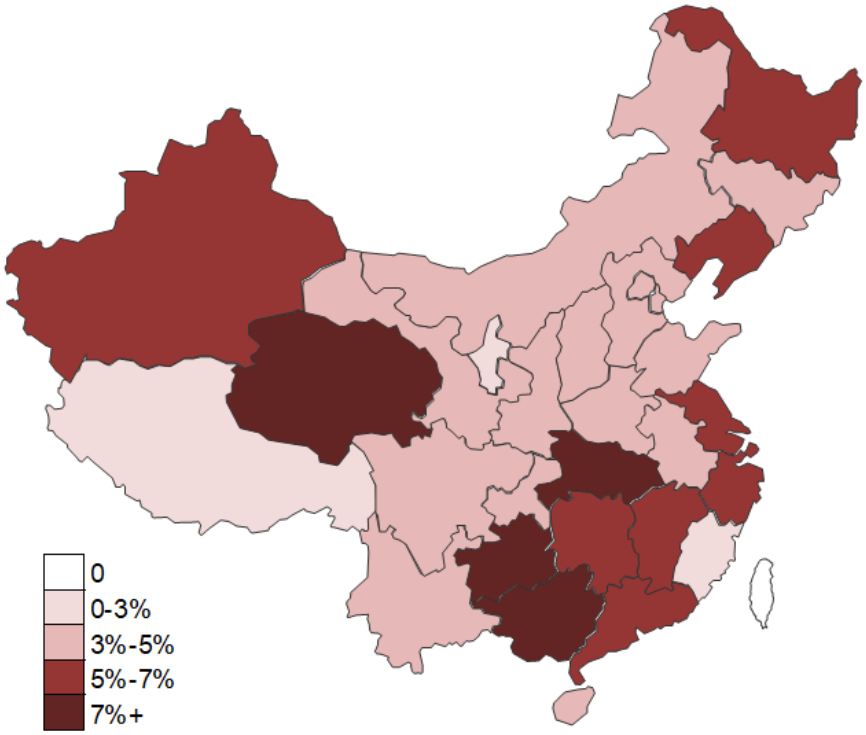

图 3.1 各省存在僵木蠕等恶意程序的单位占比情况

观测发现，健康医疗行业涉及的僵木蠕等恶意程序主要分以下四类：

- **勒索病毒**：勒索病毒通过绑架用户文件或破坏用户计算机等方式，向用户勒索数字货币，是一种会对业务系统造成恶劣影响的严重威胁。本次观测有 136 家单位存在勒索病毒风险。
- **远控木马**：此类木马进入主机后一般处于潜伏状态，但一旦活跃，可操作主机执行多样化的恶意行为，如 DDos 攻击、窃取数据、破坏数据等，甚至可以执行加密勒索，对系统可能造成重大影响。本次观测有 539 家单位存在远控木马。
- **挖矿木马**：此类木马主要目的为牟利，通过消耗失陷主机的资源，为攻击者挖取加密货币，导致用户电脑资源和性能变低。本次观测有 359 家单位存在挖矿木马。
- **捆绑软件与流氓广告**：此类恶意程序本身造成的危害不大，但其往往会成为更严重风险的跳板，例如勒索病毒可以通过捆绑软件植入主机。本次观测共有 557 家单位存在捆绑软件与流氓广告。

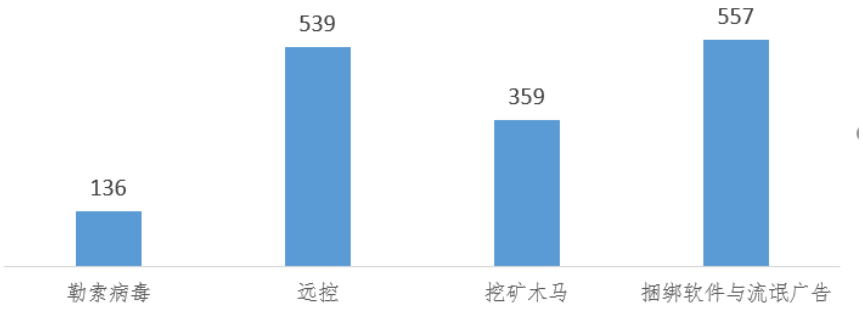

图 3.2 四类主要恶意程序涉及的单位数目

以上僵木蠕等恶意程序中，勒索病毒造成的危害与社会影响性尤为突出，本报告重点对本次观测中发现的勒索病毒的潜伏情况进行了地域分布分析。

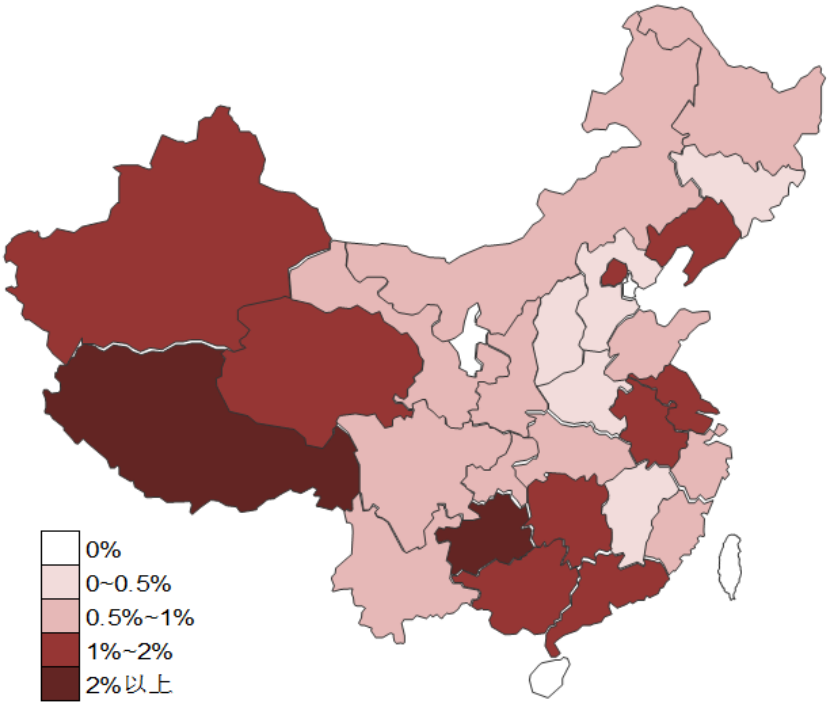

图 3.3 各省存在勒索病毒潜伏的单位占比情况

整体来看，勒索病毒潜伏比率较高的区域中，信息化程度较低或者经济发达的情况更为凸显。西藏、贵州、新疆、青海等地域，信息化程度较低，攻击成功率较高；两广、长三角、北京等经济较为发达，攻击者关注程度较高。

2.2 数据泄露事件高发，应用服务存在隐患

本报告团队梳理了部分 2019 年国外健康医疗行业安全事件，发现国外健康医疗行业安全事件中，数据泄露相关事件高发，已多于勒索病毒相关事件。数据泄露问题已是全球健康医疗行业面临的网络安全的重点问题之一。

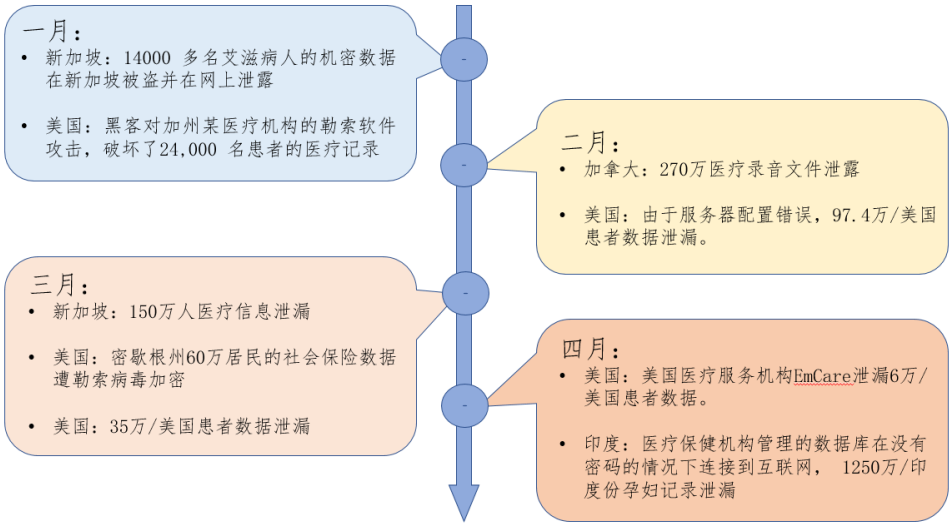

图 3.4 国外一到四月健康医疗行业安全事件梳理

本次观测发现，健康医疗行业存在大量应用服务（如数据库服务、FTP 服务、打印机服务等）暴露在公共互联网的情况，共涉及 6446 家单位。如果这些暴露的应用服务管理存在缺陷,那么攻击者从公共互联网会轻易地窃取到医疗相关数据。

应用服务存在隐患的单位在各省之间分布情况如下：

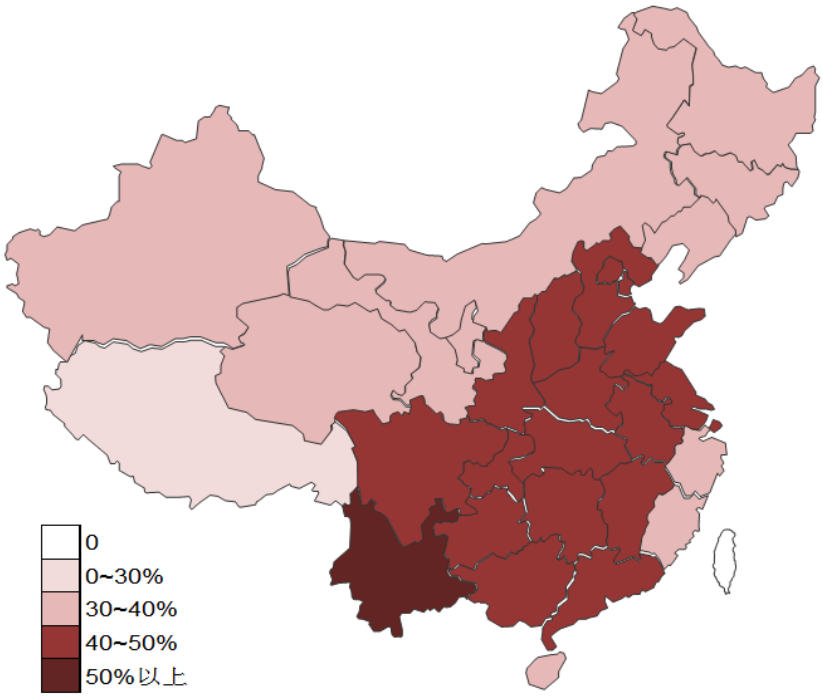

图 3.5 各省应用服务存在隐患的单位占比情况

除西藏自治区外，其余各省至少有 30%以上的单位将应用服务直接暴露在公共互联网。从分布上看，东北、西北各省与东南的福建省、浙江省和海南省略少，其余省份皆高于 40%。

2.3 网站篡改手法多变，隐式植入非法信息

根据攻击效果，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 261 家单位。按省份分布如下：

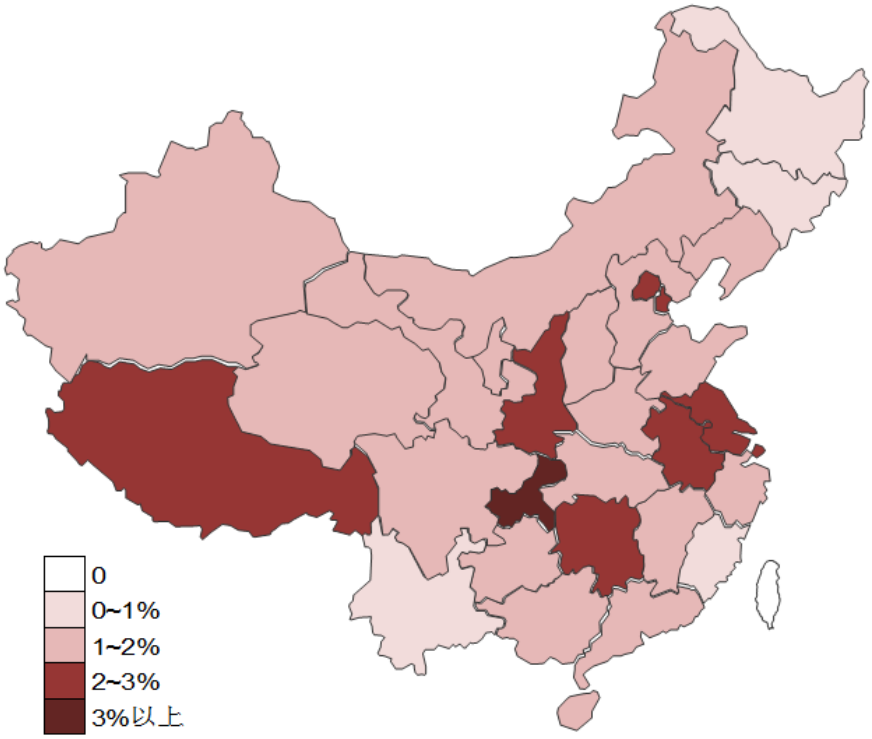

图 3.6 各省网站当前已被篡改的单位占比情况

全国总体来看都存在网站篡改现象，但主要集中分布在四片区域：分别是上海、江苏、安徽区域；北京、天津区域；陕西、重庆、湖南区域以及西藏区域。

本次观测中发现的网站篡改以隐式篡改为主，其篡改手法主要表现为以下三种：

1、寄生页面，指站点目录结构中被放入了非法页面资源，以博彩、色情站点资源为主。这些页面一般在单位站点中并无入口，寄生的主要目的是躲避观测，利用站点资源。

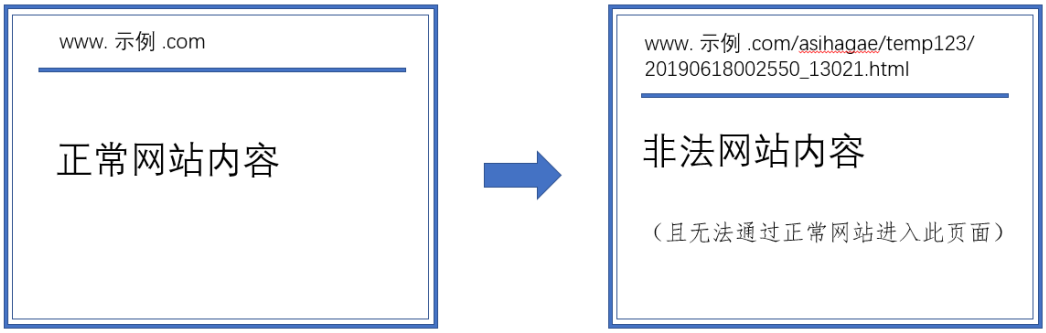

图 3.7 寄生页面篡改手法展示

图 3.8 某医院网站存在寄生页面篡改案例

2、暗链，指页面代码被放入不可显示的链接，一般为博彩、色情网站链接。暗链的主要目的是帮助非法网站在搜索引擎排名中获得更高优先级。

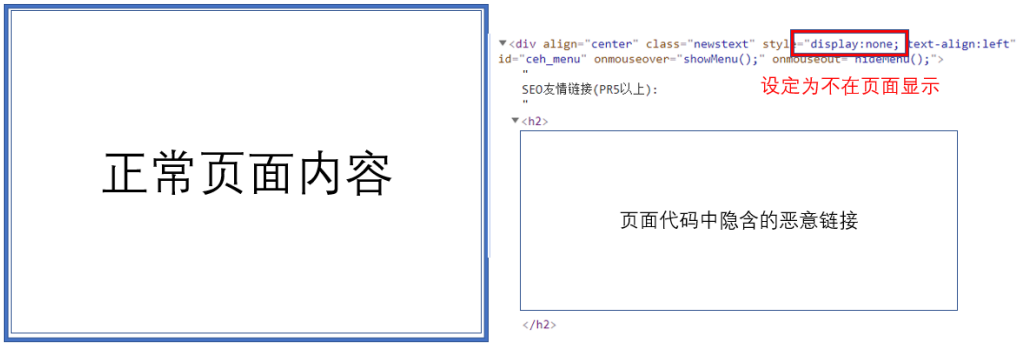

图 3.9 暗链页面篡改手法展示

图 3.10 某医院网站存在暗链页面篡改案例

3、域名恶意利用，指单位域名被用于无关内容，大部分是由于单位历史域名到期后未持续维护造成的。利用域名的主要目的也是在躲避观测的前提下使用站点资源。

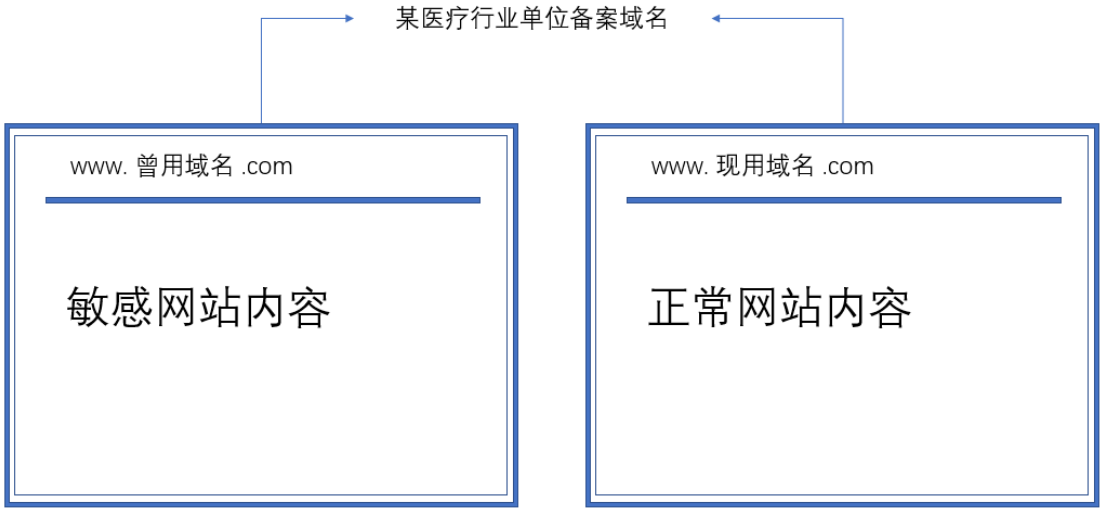

图 3.11 域名恶意利用页面篡改手法展示

图 3.12 某医院域名被恶意利用篡改案例

03

公共互联网的风险成因分析

脆弱性指资产上存在的可能被攻击者用来实施攻击的薄弱环节，即安全隐患。本报告团队基于观测结果中发现的风险点对健康医疗行业相关机构的网络资产进行了全面、客观的脆弱性评估，分析了风险存在的深度原因。

评估发现，本次观测的 15339 家单位中网络资产存在脆弱性的有 9532 家，占比 62.14%。由此可见，健康医疗行业相关机构的网络资产中存在脆弱性的情况较为普遍。

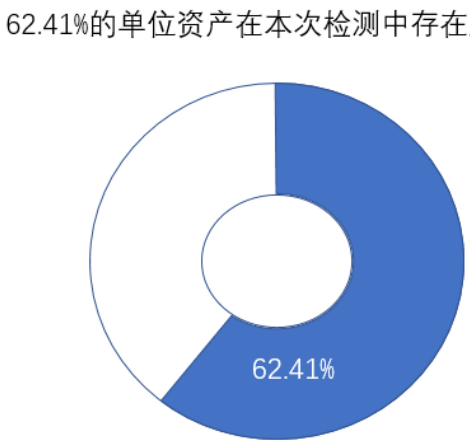

图 4.1 本次观测中存在脆弱性的单位占比

脆弱性是攻击的入口，与单位存在的安全风险息息相关。分析发现，易被利用实施攻击的脆弱性主要集中在三个方面：大量敏感的应用服务暴露在公共互联网，覆盖了 48.08%的单位；开放的高危端口上存在可被利用的高危漏洞，覆盖了

47.21%的单位；服务版本过低，存在公开漏洞，覆盖了 37.90%的单位。

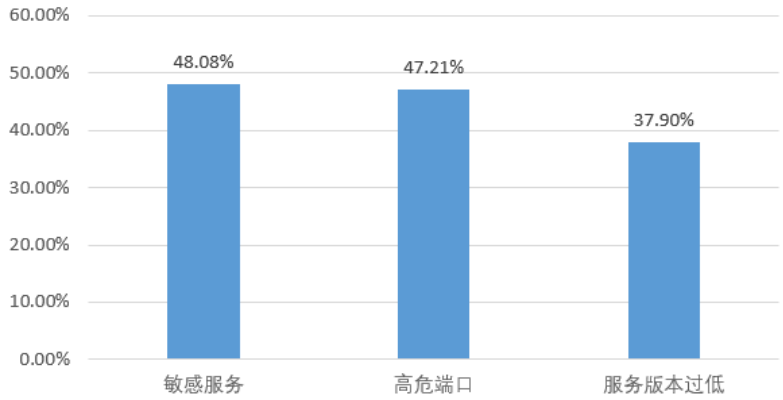

图 4.2 本次观测中存在三大脆弱性的单位占比

3.1 端口存在高危漏洞，易被僵木蠕等利用

Web 服务一般都是通过端口号来识别的。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不怀好意的人所利用，往往造成很严重的后果，比如敏感数据被窃取、服务器命令任意执行、服务器权限被非法获取等。

曾经造成重大影响的 WannaCry 勒索病毒，就是利用了 TCP 的 445 端口，以类似于蠕虫病毒的方式传播，攻击主机并加密主机上存储的文件进行勒索。自 2017 年 5 月 12 日到 5 月 15 日，WannaCry 勒索病毒共造成 150 多个国家遭受网络攻击，涉及金融、能源、医疗等行业，造成了严重的危机管理问题。

本次观测到的高危端口 top10 分布如下：

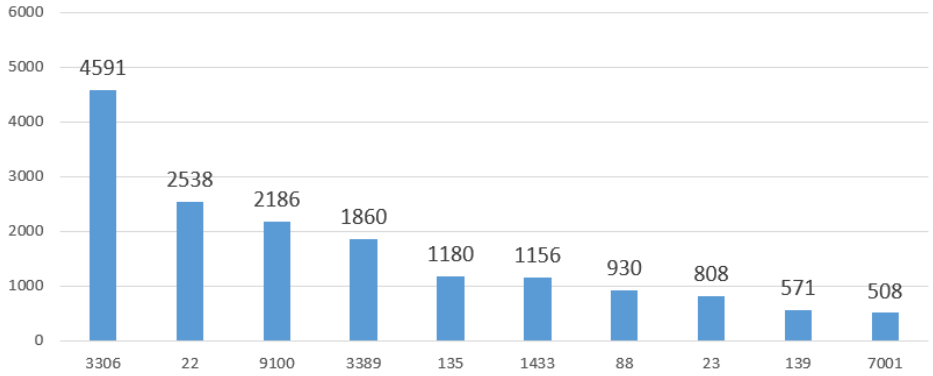

图 4.3 本次观测中涉及单位最多的十个高危端口

以作为微软操作系统远程桌面的服务端口的 3389 端口为例，2019 年 5 月 14 日微软官方发布安全补丁，修复了 Windows 远程桌面服务的远程代码执行漏洞 CVE-2019-0708。此漏洞是预先验证身份，无需用户交互（无需验证系统账户密码），即可以在目标系统上执行任意命令。这就意味着这个漏洞可以通过网络蠕虫的方式被利用，与 WannaCry 勒索病毒极为类似。

本次观测针对此漏洞进行了渗透测试，在开放 3389 端口的 1860 家单位中，有 1012 家可被利用成功，占比高达 54.40%。如果这些单位遭受利用此漏洞发起的攻击，则可能被轻易植入勒索病毒等各种恶意程序。

3.2 大量敏感服务暴露，弱口令成安全隐患

本次观测发现在公共互联网侧存在大量远程登录服务、数据库服务、FTP 服务、打印机服务等敏感服务。

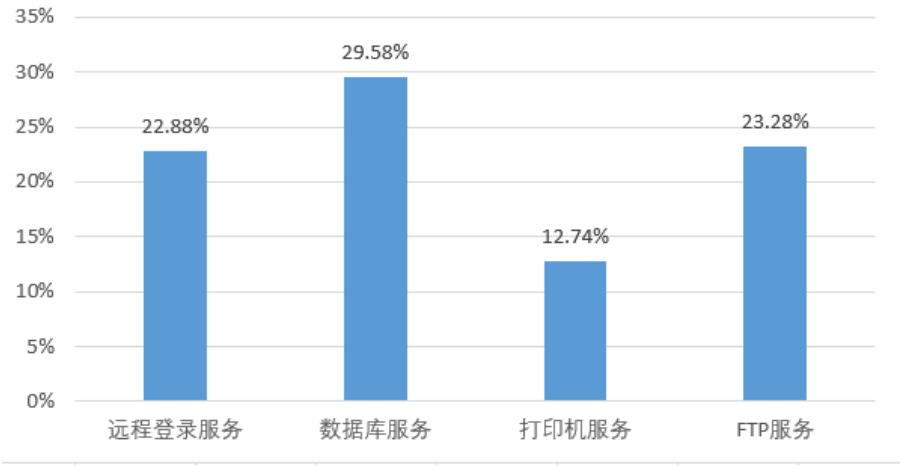

图 4.4 本次观测具体敏感服务涉及的单位占比

本次观测对暴露的应用服务中的密码情况进行了渗透测试，发现有 410 家单位存在弱口令问题。密码是网络安全的第一道屏障，攻击者一旦攻破密码，很容易通过非法登录提权至管理员权限，甚至直接渗透内网，登录内网服务器。这些单位的服务器轻则成为攻击者进行不法行为的跳板或僵尸网络的一部分，重则感染病毒，产生数据泄露，造成严重损失。

3.3 应用组件版本较低，网站篡改概率较高

应用服务组件版本过低，往往被公开漏洞所利用，存在极大的安全隐患。本次观测有 7242 家单位存在这种情况，占比 47.21%，具体服务分布如下：

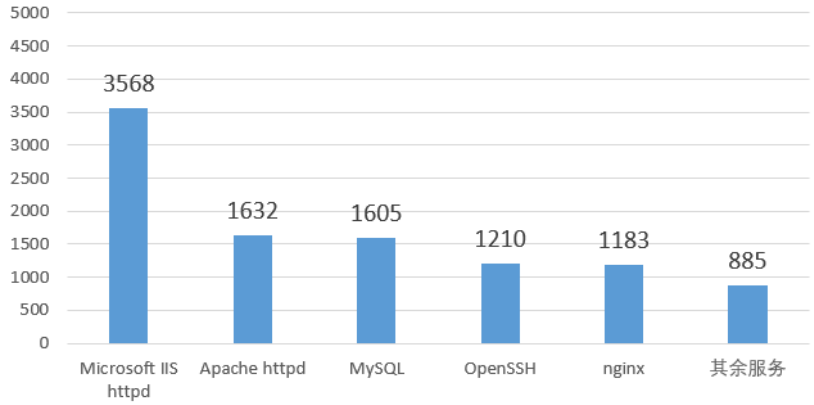

图 4.5 本次观测涉及较多单位的低版本的服务

其中，低版本的网站服务最为常见。以 Apache httpd 服务为例，本次观测中共有 2961 家单位的 Apache httpd 服务暴露在公共互联网上，其中服务版本过低的单位有 1632 家，有 55 家单位存在网站篡改，网站篡改率为 3.35%；服务版本正常的单位有 1329 家，有 22 家单位存在网站篡改，网站篡改率为 1.69%。存在低版本服务的单位网站篡改率明显高于服务版本正常的单位。

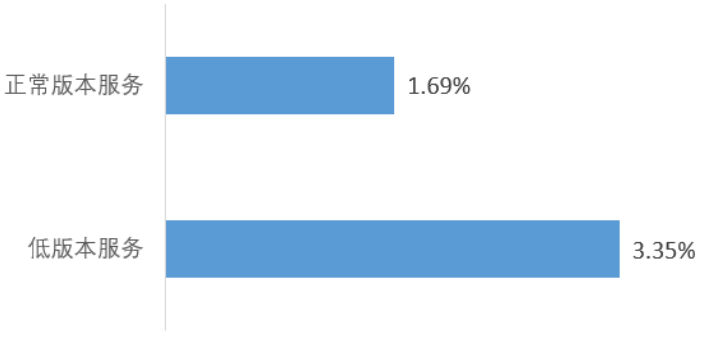

图 4.6 本次观测中服务版本对网站篡改率的影响

04

医院的网络安全现状调研

风险隐患的存在与安全防护措施的实施息息相关。为更全面地观测我国健康医疗行业网络安全现状，本报告团队基于 CHIMA 发布的《2019 医院信息安全调查报告》（以下简称《调查报告》）中的相关数据对当前医院的网络安全现状进行了分析。

《调查报告》对我国部分医院的安全建设情况进行了网络问卷调查，共回收有效问卷 400 份，医院样本总数为 389 家，覆盖 29 个省、直辖市（包含中国台湾省），医院占总参与调查机构的 97.25%。

对调查的相关数据进行分析可以发现，健康医疗行业相关机构对网络安全重视程度不够，网络安全相关工作开展不足。这就造成医疗信息系统面临的网络安全风险挑战很大，甚至导致医疗正常业务受干扰或终止、个人信息泄露和医疗数据被篡改等严重后果。主要表现在：

4.1 医院的网络安全等级保护工作普遍不足

安全防护措施的制定和实施是保证医院信息系统安全稳定运行的必要条件。国家卫生主管部门对医疗机构的信息安全等级保护工作提出了严格要求。

根据《调查报告》，至少有一个系统通过等保三级测评的受访医院共计 195 家，占比 50.13%；通过等保二级测评的受访医院共计 40 家，占比 10.28%；有实施等保工作规划

的医院有 106 家，占比 27.25%；没有开展等保工作规划的医院有 48 家，占比 12.34%。

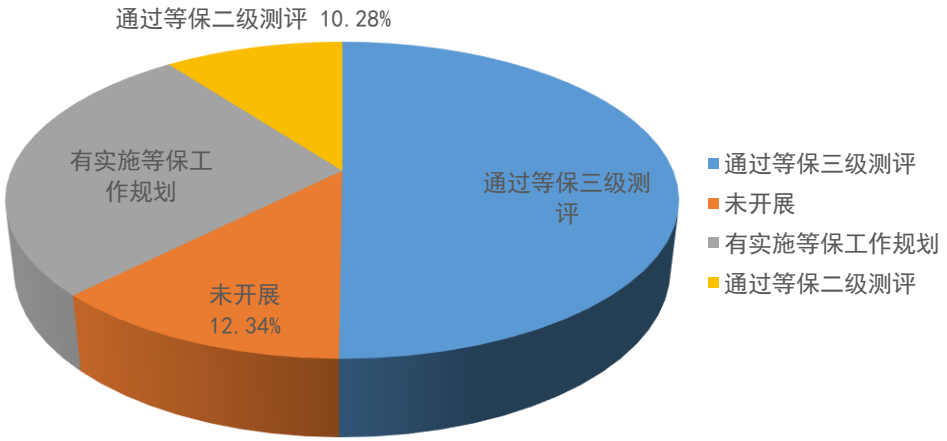

图 5.1 调研医院中等级保护开展情况分布

数据来源：CHIMA《2019 医院信息安全调查报告》

由此可见，各医院推进网络安全等级保护的工作的力度和进展存在较大差别，有些医院未开展科学、合理的系统定级工作，使系统缺乏必要的安全保障措施。等级保护有助于对系统安全进行重新梳理，发现医院系统内、外部存在的安全风险和隐患，提高网络安全防护能力，降低系统被攻击的风险，能够更加有效的保障医疗信息安全。因此，医院在信息化建设中适当提高对等级保护的侧重，有助于保障医院信息系统持续稳定安全运行。

4.2 尚未建立定期开展风险评估的工作机制

医院的网络安全等级保护要求开展周期性的网络安全风险评估工作，重点针对医疗信息系统进行渗透测试等技术评估。根据《调查报告》，本次调查中共有 37 家受访医院表示采用了定期渗透测试以评估风险，占受访医院的 9.51%。同时还有 27 家医院填写了每年定期渗透的次数，每年一次的医院有 12 家，每年两次的医院有 11 家，每年三次的医院有 1 家，每年四次的医院有 5 家。

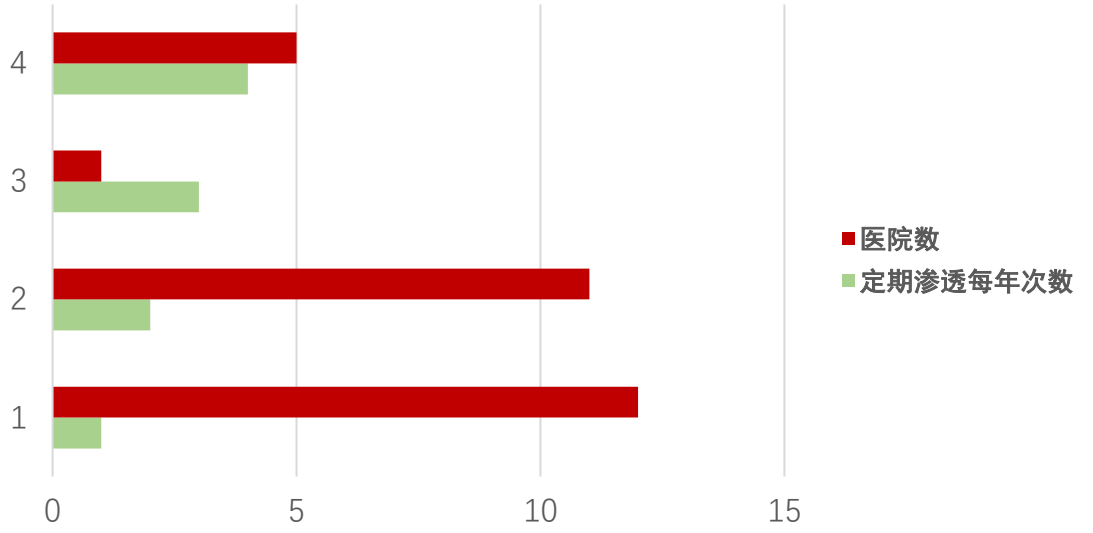

图 5.2 调研医院中定期渗透的开展情况分布

数据来源：CHIMA《2019 医院信息安全调查报告》

由此可见，绝大部分医院尚未建立对信息系统开展定期渗透测试的风险评估机制，在少数已开展定期渗透测试的医院当中，测试开展的频率偏低。定期渗透测试有助于评估信息系统抵御网络入侵的能力，当前的开展情况反映了医院对网络信息安全的评估方法不够全面、有效。

4.3 网络安全培训与应急演练预案覆盖不全

在医院内部定期开展网络安全相关培训与应急演练工作，有助于培养相关人员的安全素养和安全意识，提高相关人员的专业知识水平和处理安全事件的能力。

根据《调查报告》，此项调查共回收 198 个有效回答。在安全培训方面，有 111 位受访者表示医院会定期在信息部门内部举行网络安全培训，占比 56%；36 位受访者表示医院设置了专门的信息安全员，由他们负责进行网络安全培训，占比 18%；31 位受访者表示医院会对全体员工进行网络安全培训，占比 16%；20 位受访者表示没有相关培训，占比 10%。

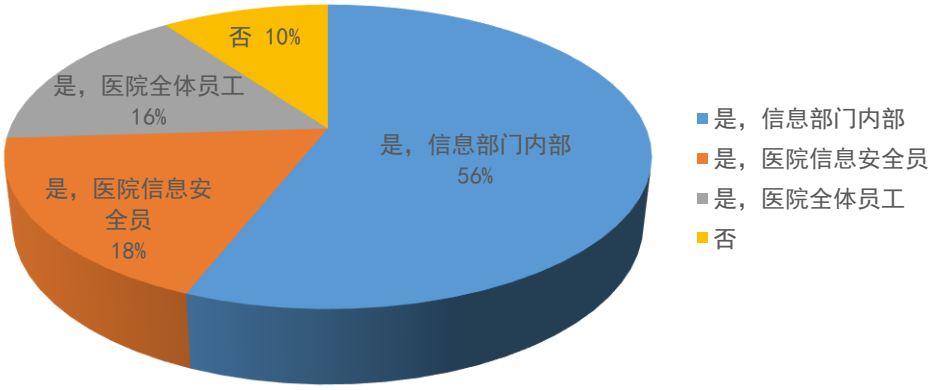

图 5.3 医院信息安全培训情况

数据来源：CHIMA《2019 医院信息安全调查报告》

在应急演练方面，选择信息部门内部参加的定期网络安全应急演练的共计 93 位受访者，占比 47%；选择医院全体员工参加的定期网络安全应急演练的共有 42 位受访者，占比 21%；选择仅有医院设立的信息安全员参加的定期网络安全应急演练有 36 位受访者，占比 18%；回答医院没有定期组织网络安全应急演练的有 27 位受访者，占比 14% 。

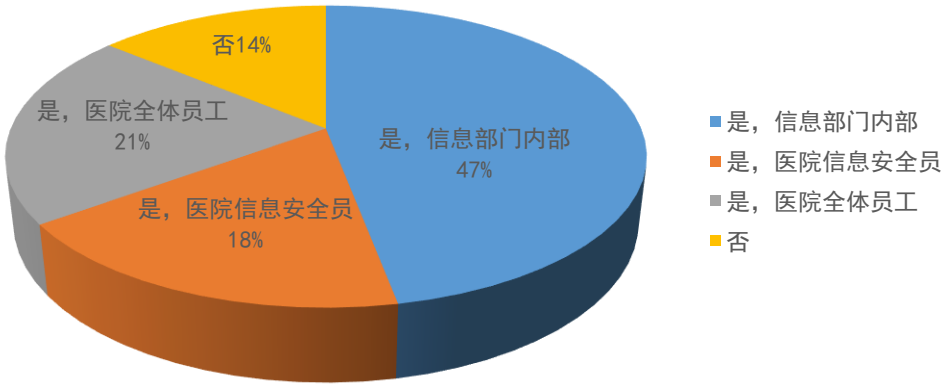

图 5.4 调研医院中应急演练的开展情况

数据来源：CHIMA《2019 医院信息安全调查报告》

由此可见，目前各医院开展网络安全培训和应急演练工作的覆盖面不足，近半数的医院仅在信息部门内部定期开展网络安全培训和应急演练工作，设置专门信息安全员的医院不足 20%，还有部分医院完全没有进行安全培训和应急演练。这既不利于提高工作人员的安全意识，也无法有效保障医院信息系统的安全。

05

安全工作思路与建议

5.1 提高政治站位，统一思想认识

健康医疗行业事关人民福祉和国家安全，健康医疗行业相关机构应提高政治站位，统一思想，充分认识到做好健康医疗行业网络数据安全保障工作的重要性和紧迫性，坚决贯彻落实习近平总书记有关数据安全重要批示指示精神，坚决做好大数据安全与医疗信息化稳定发展的保障工作。

5.2 加强政策引导，完善防护体系

保障健康医疗网络安全是卫生事业改革和发展的重要内容。为加强健康医疗领域网络安全体系建设，保障医疗领域信息化的顺利发展，不断满足人民群众多层次、多样化的健康需求，亟需完善健康医疗领域网络安全体系建设，提升健康医疗领域网络安全防护能力，为持续推进健康医疗信息化安全稳定发展保驾护航。

5.3 强化标准引领，规范行业发展

健康医疗行业网络安全标准化工作作为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。为全面切实推进健康医疗领域的网络安全防护工作整体、规范，科学、有序的开展，亟需健全完善健康医疗行业的网络安全标准化体系建设。

5.4 突出能力建设，形成长效机制

健康医疗行业相关机构应加强自身网络数据安全综合保障能力建设，继续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，形成长效机制：

- 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；
- 定期开展风险评估工作，评估系统抵御网络入侵的防护能力，发现潜在的安全隐患；
- 建立网络安全专业团队，定期进行安全培训及应急演练，提升团队安全意识和风险应对能力；
- 充分发挥第三方安全机构的专业支撑能力，采用安全最佳实践，保障医疗信息化的安全发展。

特别声明：

本观测报告仅供技术研讨与参考分析，多有纰漏与不足之处，欢迎各领导专家指导修正，共同推进健康医疗行业的网络安全防护与大数据安全工作。

附录一：网络安全术语解释

- 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的，以处理信息和数据为目的的系统。

- 资产

资产指对组织具有价值的信息或资源，是安全策略保护的对象。

- 资产价值

资产价值指资产的重要程度或敏感程度的表征。资产价值是资产的属性，也是进行资产识别的主要内容。

- 威胁

威胁指可能导致对系统或组织危害的不希望事故潜在起因。

- 脆弱性

脆弱性是指可能被威胁所利用的资产或若干资产的薄弱环节，即安全隐患。

- 恶意程序

恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。

- 病毒

病毒是通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的的恶意程序。

- 勒索软件

勒索软件是黑客用来劫持用户资产或资源并以此为条件向用户勒索钱财的一种恶意程序。勒索软件通常会将用户

数据或用户设备进行加密操作或更改配置，使之不可用，然后向用户发出勒索通知，要求用户支付费用以获得解密密码或者使系统恢复正常运行的方法。

- 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在的缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。常见漏洞有 SQL 注入漏洞、弱口令漏洞、远程命令执行漏洞、权限绕过漏洞等。

- 蠕虫

蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意程序。按照传播途径，蠕虫可进一步分为邮件蠕虫、即时消息蠕虫、U 盘蠕虫、漏洞利用蠕虫和其他蠕虫 5 类。

- 网页篡改

网页篡改是恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容。

附录二：风险量化评估细则

1、 简介

量化评估的得分包括两部分：脆弱性分和威胁分。

脆弱性分采用《信息安全风险评估规范》中提到的评估方法进行计算，威胁分采用威胁情报和网站篡改的数据按可能性、按频率进行计算。

具体操作流程是：

（1）将端口当作最细粒度资产，根据漏洞扫描数据计算 Port 脆弱性分；

（2）结合端口上服务的资产价值分，由 Port 脆弱性分汇总到 IP 脆弱性分；

（3）计算集成了威胁情报分的 IP 安全分；

（4）由 IP 安全分汇总到单位安全分；

（5）计算集成了网站篡改分后的单位安全分。

2、 量化评估流程

2.1 计算 Port 脆弱性分

总分 1000 分，分别计算漏洞、服务版本低、高危端口、特定服务暴露在大网四个部分的脆弱性分，然后加权汇总。

（1）漏洞，分高危、中危、低危三种漏洞，分别对应 level 的值 1、2、3，即$\boldsymbol{value_{level}}$代表每种漏洞的价值分，且 0<$\boldsymbol{value_{level}}$<1，$\boldsymbol{cnt_{level}}$代表每种漏洞的数量，则

$$\boldsymbol{score_1} = \begin{cases} \mathbf{1000} - \mathbf{1000} * \min\left(\mathbf{1}, \sum_{level=1}^{3} (\log_m(cnt_{level} + n) * value_{level})\right), \\ cnt_{level} > 0, m > 0 且 m \neq 1, n \geq 1 \\ \mathbf{1000}, \sum cnt_{level} = 0 \end{cases}$$

其中，m、n 是根据$\boldsymbol{cnt_{level}}$和总体分数分布确定的参数。

（2）服务版本低，假设因为服务版本低而匹配到的公开的漏洞个数为cnt_{cve}，则

$$score_2 = \begin{cases} 1000 - 1000 * \min(1, \log_m(cnt_{cve} + n)), & cnt_{cve} > 0, m > 0 且 m \neq 1, n \geq 1 \\ 1000, & cnt_{cve} = 0 \end{cases}$$

其中，m、n 是cnt_{cve}和总体分数分布确定的参数。

（3）高危端口，假设高危端口标识为$flag_{danger}$，则

$$score_3 = \begin{cases} 0, & flag_{danger} = 1 \\ 1000, & flag_{danger} = 0 \end{cases}$$

（4）特定服务暴露在大网，假设存在标识为$flag_{special}$，则

$$score_4 = \begin{cases} 0, & flag_{special} = 1 \\ 1000, & flag_{special} = 0 \end{cases}$$

此处所指的特定服务类型包括远程登陆服务（主要包括 microsoft-ds、ms-wbt-server、ssh、telnet、vnc 等）、数据库服务（主要包括 ibm-db2、ms-sql-s、mysql、oracle、postgresql、redis 等）、文件传输服务（主要包括 ftp 等）、打印机服务（主要包括 jetdirect 等）。

以上四部分分数权重占比分别为α_1，α_2，α_3，α_4（$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 1, \alpha_1 > 0, \alpha_2 > 0, \alpha_3 > 0, \alpha_4 > 0$），因此每个 Port 的总分

$$score_{port} = \alpha_1 * score_1 + \alpha_2 * score_2 + \alpha_3 * score_3 + \alpha_4 * score_4$$

2.2 由 Port 脆弱性分汇总到 IP 脆弱性分

在将 Port 分汇总到 IP 分之前，首先需要考虑每个 Port 所对应的服务的资产价值，即不同类型服务所对应的资产价值分是不同的。在对不同服务计算资产分数时采用国标中推荐的方法，分为保密性价值、完整性价值、可用性价值三部分分别计算得分，最后再进行加权汇总。

保密性价值

是否可公开	可公开	组织内可公开	不可公开	不可公开	不可公开
秘密重要性			一般性秘密	重要秘密	最重要秘密
泄露损失	无损害	轻微损害	一般损害	严重损害	灾难性损害，决定组织根本利益
分值	1	2	3	4	5

完整性价值

破坏后对组织影响	可忽略	轻微影响	一般影响	重大影响	无法接受的影响
破坏后对业务冲击程度	可忽略	冲击轻微	冲击明显	冲击严重高	冲击重大
是否容易弥补	易弥补	易弥补	可弥补	较难弥补	难弥补
分值	1	2	3	4	5

可用性价值

可用度占正常工作时间的百分比	低于四分之一	四分之一以上	70%以上	90%以上	接近百分之百
系统允许中断时间	大于一个小时	小于一个小时	小于半个小时	小于 10 分钟	不允许中断
分值	1	2	3	4	5

资产总分值$\boldsymbol{value_{asset}}$=($\boldsymbol{\beta_1}$*完整性价值+$\boldsymbol{\beta_2}$*保密性价值+$\boldsymbol{\beta_3}$*可用性价值)/5,其中$\boldsymbol{\beta_1+\beta_2+\beta_3=1,\beta_1>0,\beta_2>0,\beta_3>0}$。

每个 IP 的得分由该 IP 上所有端口的得分汇总得到。有两种汇总方法，一种是加权平均，一种是在 IP 的总分上直接减 Port 的减分项分数。考虑到减分方案更能突出 IP 上的风险情况，因此选择第二种方法。

每个 IP 总分为

$$\boldsymbol{score_{ip}=\max(0,\quad 1000-\sum((1000-score_{port})*value_{asset}))}$$

2.3 计算集成了威胁情报分的 IP 安全分

以上计算的 IP 脆弱性分是指 IP 在风险脆弱性方面的得分，我们还有一部分从威胁情报中获取的数据计算了某 IP 访问病毒、木马等恶意程序相关域名的次数。这一般代表该 IP 可能感染了对应病毒、木马等。设某 IP 共访问了恶意程序的次数为$\boldsymbol{cnt_{threat}}$，则该 IP 的威胁情报分数为

$$\boldsymbol{score_{threat}=\begin{cases}\max(0,\quad 1000-1000*\log_m(cnt_{threat}+n)),\ \mathrm{cnt_{threat}}>0,m>0且m\neq 1,n\geq 1\\ 1000,\ \ cnt_{threat}=0\end{cases}}$$

其中,m、n 是根据$\boldsymbol{cnt_{threat}}$和总体分数分布确定的参数。

因此 IP 的安全分为

$$\boldsymbol{score_{final_{ip}}=\max(0,score_{ip}-(1000-score_{threat}))}$$

2.4 由 IP 安全分汇总到单位安全分

每个单位有一个或多个 IP，将 IP 分汇总到单位分的计

算采用扣分的方式。每个 IP 可能被一个或多个单位使用。被多个单位使用的 IP 其风险值给单位带来的损失一般较小，因此在计算这类 IP 的扣分分数时可以除以该 IP 的共享单位个数$\boldsymbol{cnt_{shared}}$。

每个单位总分为

$$\boldsymbol{score_{company}} = \mathbf{max}(\mathbf{0},\ \mathbf{1000} - \sum(\left(\mathbf{1000} - \boldsymbol{score_{final_{ip}}}\right) * \boldsymbol{m}/\ \boldsymbol{cnt_{shared}})),\quad \boldsymbol{m} > \mathbf{0}$$

其中，m 是根据$\boldsymbol{cnt_{shared}}$和总体分数分布确定的参数。

2.5 计算集成了网站篡改分后的单位安全分

网站篡改分是由检测出的网站篡改的相关数据计算的。由于网站篡改是基于 url 的，url 对应到域名，域名再对应到单位，因此网站篡改分直接基于单位计算。已知每个域名最近七天的总访问量为$\boldsymbol{cnt_{domain}}$，每个域名检测出的篡改页面 url 数为$\boldsymbol{cnt_{url}}$，则每个域名需要扣除的篡改分的系数为

$$\boldsymbol{parm_{domain}} = \begin{cases} \mathbf{log}_{\boldsymbol{l}}\left((\boldsymbol{cnt_{domain}} + \boldsymbol{m}) * \mathbf{log}_{\boldsymbol{p}}(\boldsymbol{cnt_{url}} + \boldsymbol{n}) + \boldsymbol{k}\right), \\ \boldsymbol{cnt_{url}} > \mathbf{0}, \boldsymbol{m} \geq \mathbf{1}, \boldsymbol{n} \geq \mathbf{1}, \boldsymbol{k} \geq \mathbf{1}, \boldsymbol{l} > \mathbf{0}\text{且}\boldsymbol{l} \neq \mathbf{1}, \boldsymbol{p} > \mathbf{0}\text{且}\boldsymbol{p} \neq \mathbf{1} \\ \mathbf{0}, \quad \boldsymbol{cnt_{url}} = \mathbf{0} \end{cases}$$

其中，m、n、l、k、p 是根据$\boldsymbol{cnt_{domain}}$、$\boldsymbol{cnt_{url}}$和总体分数分布确定的参数。

每个单位的篡改分为

$$\boldsymbol{score_{company_{distort}}} = \mathbf{max}(\mathbf{0},\quad \mathbf{1000} - \mathbf{1000} * \sum \boldsymbol{parm_{domain}})$$

每个单位的最终安全分为

$$\boldsymbol{score_{company_{final}}} = \boldsymbol{score_{company}} - \boldsymbol{\alpha} * \left(\mathbf{1000} - \boldsymbol{score_{company_{distort}}}\right),\ \mathbf{0} \leq \boldsymbol{\alpha} \leq \mathbf{1}$$

其中，$\boldsymbol{\alpha}$根据网站篡改分数占总分数的比重确定。