产业互联网安全观测：医疗行业安全风险分析

郑　威　中国信通院安全所

产业互联网安全观测：医疗行业安全风险分析

一、产业互联网的安全背景与环境分析

二、产业互联网安全实验室与观测平台

三、健康医疗行业的网络安全观测报告

一、产业互联网的安全背景与环境分析

1月，德国

包括总理和总统在内的多达**1000+名政界人士和名人**遭信息泄露，内容包括私人地址、手机号码、聊天记录和信用卡号码。

3月，俄罗斯

攻击者使用IoT设备发动攻击，并伪造钓鱼电子邮件，对**50多家大型企业**的人员进行勒索攻击。

3月，美国

某健康医疗公司，安全证书失效，导致服务器无密码保护，**每天泄漏数千张**医生处方、医疗记录信息。

5月，日本

电商网站遭黑客攻击，**逾46万客户**的大量个人敏感信息，存在批量拖库风险，造成数据安全事件。

7月，委内瑞拉

首都及10余个州，再次遭遇大范围停电，政府称其水电系统受到了网络电磁攻击，影响到**数百万人**。

- **习总书记讲话：**要树立正确的网络安全观，加快构建关键信息基础设施安全保障体系，**全天候 全方位 感知网络安全态势，增强网络安全防御能力。**
- **《网络安全法》第五十二条：**负责关键信息基础设施安全保护工作的部门，应当**建立健全本行业、本领域的网络安全 监测预警和 信息通报制度**，并按照规定报送网络安全监测预警信息。
- **《国家网络空间安全战略》发布：**明确九大战略任务，坚持技术和管理并重，着眼**识别、防护、检测、预警、响应、处置** 等6个环节，**“建立政府、行业与企业的网络安全信息 有序共享机制”。**
- **工业和信息化部：**《公共互联网网络安全 威胁监测与处置办法》（网安函〔2017〕202号），**强调公共互联网的 网络安全威胁监测 与处置工作，建立国家级的威胁信息共享平台与应急指挥平台。**
- **网络安全等级保护2.0《网络安全等级保护测试评估技术指南》等系列GB/T标准**

二、产业互联网安全实验室与观测平台

产业互联网安全观测平台-医疗

产业互联网安全实验室出品

2019年07月26日 星期五 16 : 48 : 28

量化评估与总结

行业资产盘点

安全隐患识别

风险情报观测

CAICT 中国信通院 安全所　腾讯安全 Tencent Security　POWERED BY PENROSE


产业互联网安全观测平台-医疗
产业互联网安全实验室出品
2019年07月25日
星期四
21 : 21 : 17
安全隐患识别
15,339家
当前检测范围
9,532家
在公共互联网发现存在安全隐患
识别公共互联网上的敏感服务
远程登录服务 3510
数据库服务 4539
FTP服务 3571
打印机服务 1954
观测公共互联网中的开放高危端口
3306端口 4591
22端口 2538
9100端口 2186
3389端口 1860
135端口 1180
感知在公共互联网下的低版本应用服务
Microsoft IIS 3568
Apache httpd 1632
MySQL 1605
OpenSSH 1210
nginx 1183
最近观测到的具体安全隐患
xxx医院ip:xx.xx.xx.xx数据库暴露，且存在弱密码
xxx医院ip:xx.xx.xx.xx存在高危端口3389，可被漏洞利用
xxx医院ip:xx.xx.xx.xx上OpenSSH版本过低，可被漏洞利用
xxx医院ip:xx.xx.xx.xx存在网站目录信息泄露
xxx医院ip:xx.xx.xx.xx远程登录暴露，且存在弱密码
数据库服务暴露
*****医院
2019-7-5
打印机服务暴露
*****医院
2019-7-19
高危端口暴露
*****医院
2019-7-12
南海诸岛
CAICT 中国信通院 安全所
腾讯安全 Tencent Security
POWERED BY PENROSE

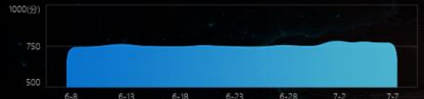
产业互联网安全观测平台-医疗

产业互联网安全实验室出品

2019年07月26日 星期五 16 : 53 : 32

医疗行业风险量化评估

指数趋势



各省量化评估分布

低风险	2
一般风险	6
较大风险	18
重大风险	5

主要风险情报态势

勒索病毒	136
远控	539
挖矿木马	359
网站被篡改	261

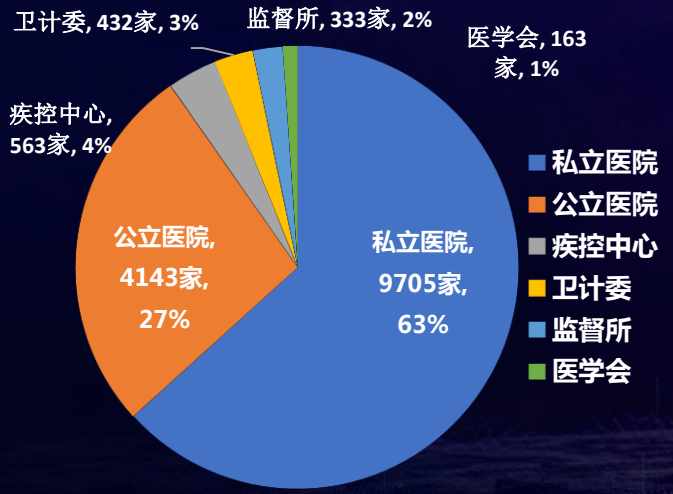
最近观测到的具体威胁

- xxx医院网站存在被篡改
- xxx医院ip:xx.xx.xx.xx疑似存在挖矿恶意软件
- xxx医院ip:xx.xx.xx.xx疑似存在勒索病毒恶意软件
- xxx医院ip:xx.xx.xx.xx疑似存在远控恶意软件
- xxx医院ip:xx.xx.xx.xx疑似存在广告恶意软件

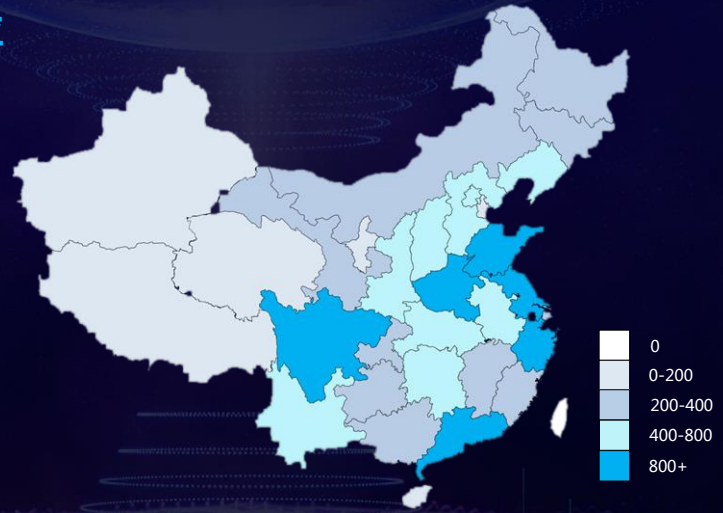
CAICT 中国信通院 安全所 | 腾讯安全 Tencent Security | POWERED BY PENROSE

三、健康医疗行业的网络安全观测报告

观测范围：全国31省，共计15339家单位



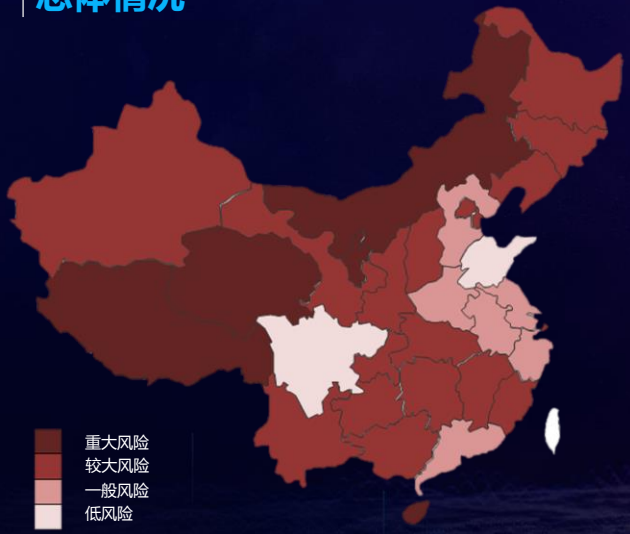
观测范围：职能划分



观测范围：地域划分

山东、河南、江苏、四川、浙江、广东，6省的单位分布较多，均为800+单位

总体情况



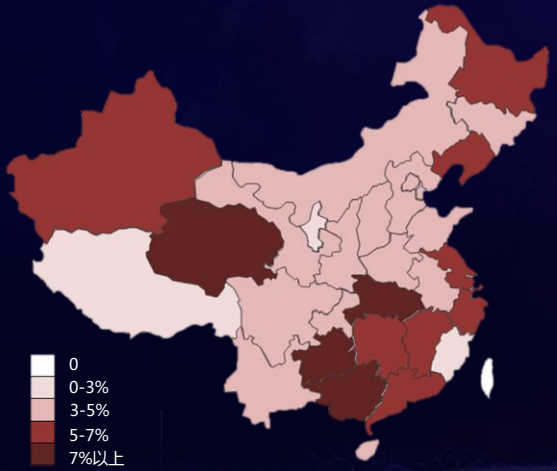
平台观测15339家单位，其中9532家发现了安全隐患，1460家已发现安全风险，且可实施攻击入侵。

- **重大风险，5省：**青海、海南、内蒙古、西藏、宁夏；
- **较大风险，18省：**北京、上海、重庆、天津、福建、山西、甘肃、贵州、黑龙江、湖北、湖南、江西、吉林、辽宁、陕西、云南、广西、新疆；
- **一般风险，6省：**浙江、江苏、河南、广东、安徽、河北；
- **低风险，2省：**山东、四川。

风险级别	对应分数段
重大风险	0-500分
较大风险	500-800分
一般风险	800-900分
低风险	900-1000分

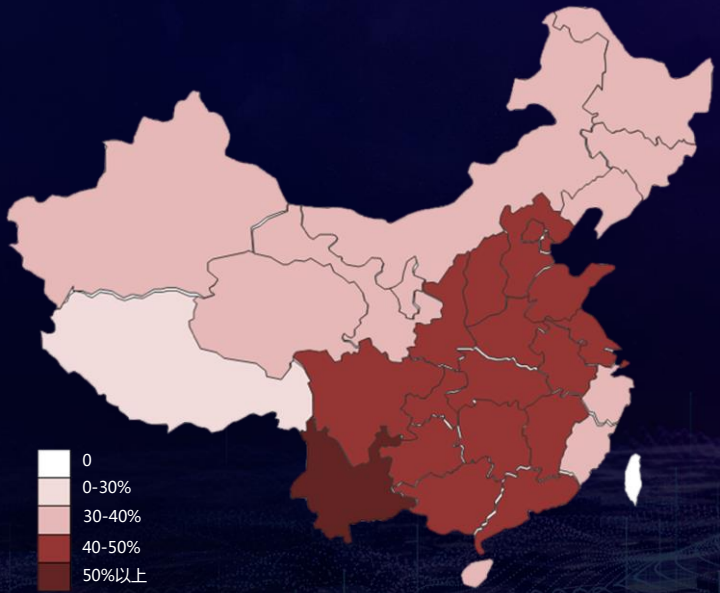
行业总体788分，处于“较大风险”级别

风险一：僵木蠕等问题严峻，勒索病毒威胁严重



僵木蠕等恶意程序的分布覆盖了全国31省，青海、广西、贵州、湖北，4省占比最高。

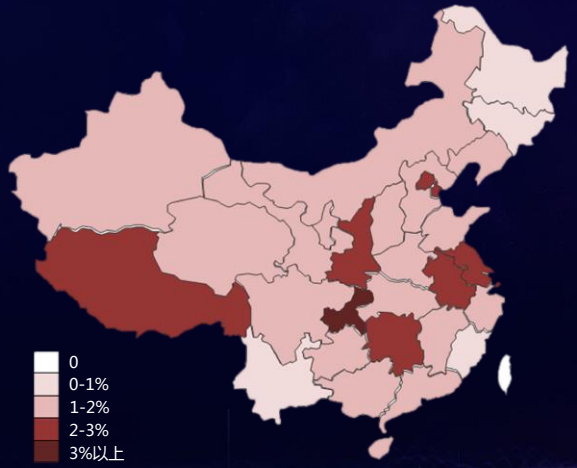
风险二：数据泄露事件高发，大量应用服务公网暴露



大量的应用服务（数据库、中间件、FTP等），暴露在公共互联网，共涉及6446家单位，各省应用服务，存在安全隐患的单位占比情况：

- 云南，占比50%以上；
- 中部、南部各省，普遍占比40-50%；
- 东北、西北、东南的福建、浙江，海南占比30-40%；
- 西藏，占比30%以下。

风险三：网站篡改手法多变，隐式植入非法信息



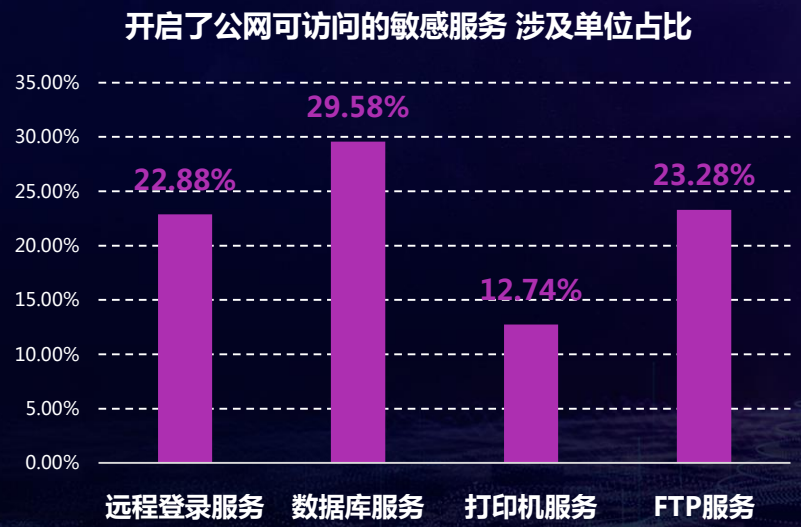
各省网站当前已被篡改的单位占比情况，主要集中在 北京、天津、上海、江苏、安徽、重庆、陕西、湖南、西藏等9省。

1. **寄生页面**，站点目录结构中植入非法页面资源，博彩、色情为主。
2. **暗链**，页面代码植入不可显示的链接，博彩、色情、广告为主。
3. **域名恶意利用**，指单位域名被用于无关内容，常因历史域名服务到期后，未持续维护造成。

原因一：端口存在高危漏洞，易被僵木蠕等利用

- 普遍存在 数据库、SSH、打印机服务远程可访问的情况；
- 以3389远程桌面严重漏洞（CVE-2019-0708）为例，在开放3389端口的1860家单位中，有1012家可被成功攻击利用，设备远程可控，占比高达54.40%。

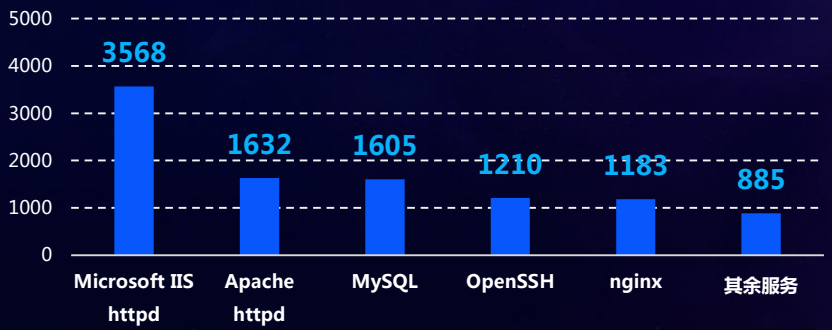
原因二：大量敏感服务暴露，弱口令成安全隐患



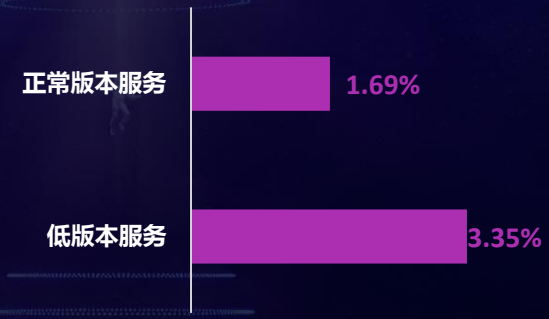
- 公共互联网侧，存在大量远程登录服务、数据库服务、FTP服务、打印机服务等敏感服务。
- 对暴露的应用服务的登入密码，进行爆破测试，**发现有410家单位存在弱口令问题，导致设备远程可控。**

原因三：应用组件版本较低，网站安全风险突出

不同应用组件的低版本问题分布类型

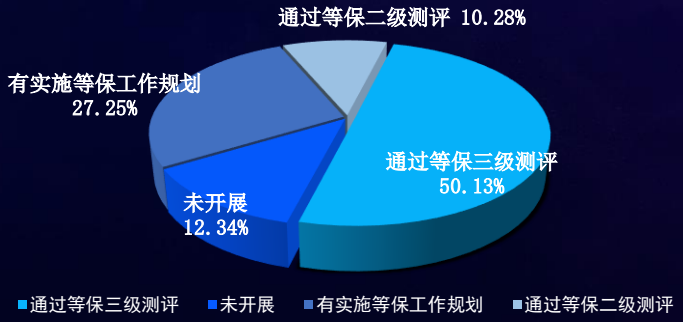


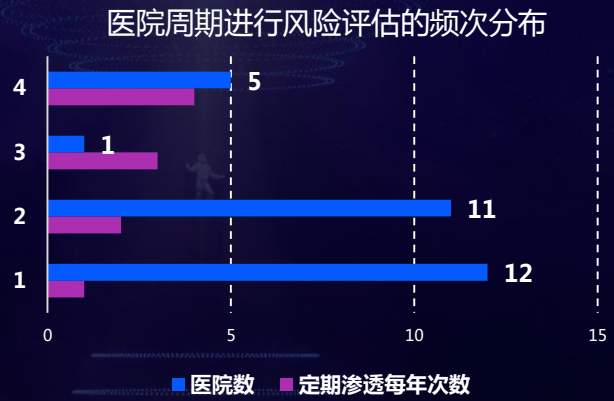
低版本问题对网站被篡改的影响



- 观测发现，行业内普遍存在应用组件低版本的问题， **共计7242家单位，占比47.21%**
- 存在低版本服务的单位网站篡改率，约为服务版本正常单位的**两倍。**

原因四：安全意识不足，等保与风险评估工作不到位





抽样调查医院，有效样本389家，覆盖29个省

- 至少有1个系统通过等保三级测评的受访医院共195家，占比50.13%；通过等保二级测评的共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%；**未开展等保工作规划的医院有48家，占比12.34%。**
- 仅37家受访医院表示，开展了风险评估工作，**占比9.51%。**

  每年1次的医院有12家，每年2次的医院有11家，每年3次的医院有1家，每年4次的医院有5家，其余均反馈为非周期评估。


对当前医疗信息化安全系统进行全面体检，定位安全问题，排除安全隐患
1.摸清家底，排查隐患
加强医疗网络信息安全技术团队培训，全面提升安全防御意识和团队素养
2.强化意识，培养团队
3.构建防御体系
选择专业的医疗网络信息安全解决方案，建设安全防御体系，降低安全风险
4.应急演练、事件应对
定期进行网络信息安全检查及安全防御演练，提升重大威胁应急响应能力
5.应对风险、监管合规
建立面向行业的应急响应协同机制，及时预警联防共治，携手应对网络风险

CSS 互联网安全领袖峰会 Cyber Security Summit

Tencent 腾讯 | 腾讯安全

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

感 谢 聆 听

CSS 互联网安全领袖峰会 Cyber Security Summit

Tencent 腾讯 | 腾讯安全

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

感 谢 聆 听

CSS 互联网安全领袖峰会 Cyber Security Summit

Tencent 腾讯 | 腾讯安全

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

感 谢 聆 听