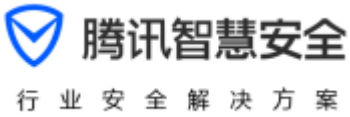
医疗互联网服务敏感数据泄露风险调查报告



1、概要

随着互联网、大数据、云计算技术的快速发展，我国医疗机构的信息化程度越来越高，逐步向数字化医疗、智慧医疗发展。新型技术的使用必然会带来新的安全风险。此外，医疗数据的高价值特性，吸引大量攻击者尝试通过窃取、买卖医疗敏感数据牟取暴利。据悉，医疗敏感数据在暗网中的交易价格可达信用卡数据的 10 倍。

腾讯智慧安全以安全大数据及第三方授权或公开的信息和数据为基础，抽样分析了国内具有一定影响力的线上医疗服务平台的业务情况，并结合网络安全威胁情报、黑灰产业链等情报信息，对国内医疗数据泄露风险做了综合性的评估。评估发现国内线上医疗服务平台存在的业务安全风险比较突出，可能会导致大量敏感的医疗数据泄露，主要问题如下：

1）线上医疗服务平台普遍存在多种逻辑漏洞，可能导致患者身份、就诊信息等敏感数据泄露。

2） 医疗互联网资产敏感端口开放较多，核心业务资产直接对外暴露，存在被入侵、攻击的风险。

2、线上医疗服务总体情况

随着我国互联网+医疗的发展，国内越来越多的医院通过手机 APP、网站、第三方医疗服务平台等形式提供了网上预约挂号、网上缴费、网上查询报告等多项线上医疗服务。

我们调查发现，近 87%的医院提供了较成熟的线上医疗服务。其中超过 60% 的医院的线上医疗服务由第三方医疗平台提供。而第三方医疗服务平台会同时为多家医院提供线上挂号预约、体检预约以及医生咨询等服务。

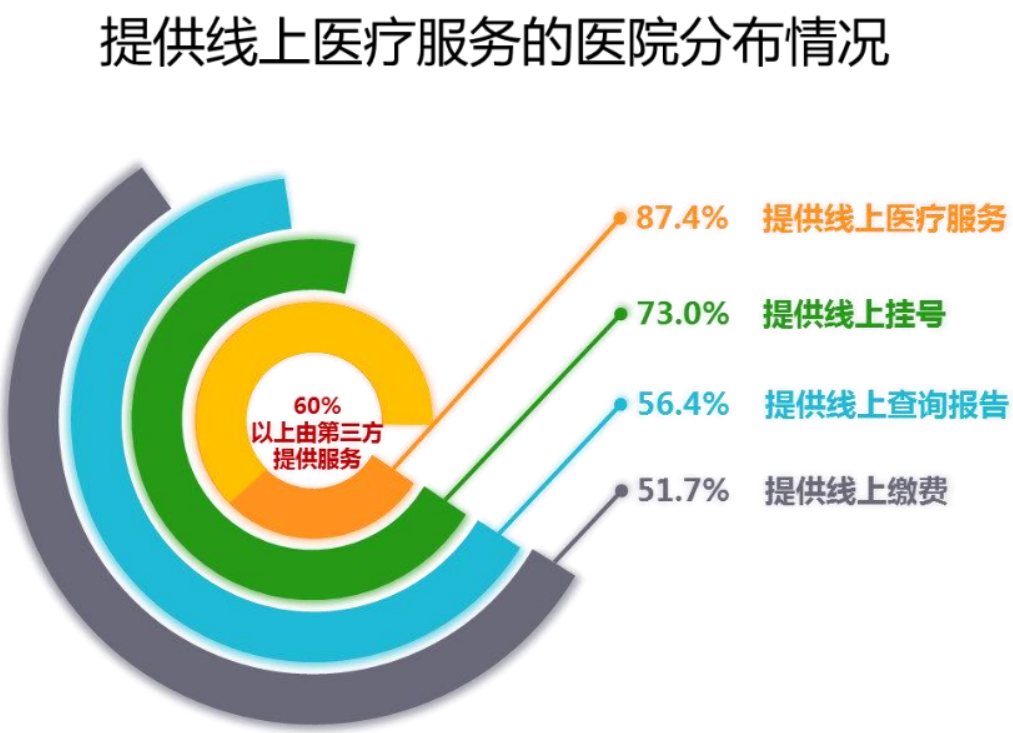


图 2-1　提供线上医疗服务的医院分布情况

3、线上医疗服务面临数据泄露风险

医疗业务系统存在的业务漏洞、敏感端口开放等安全问题，会给未授权访问和黑客入侵渗透带来极大的便利，从而增加医疗数据的安全风险。

从美国医疗数据泄露的来源可以看出，除了内部人员窃取/丢失数据等内因外，更多的是来自外部的黑客渗透入侵、未授权访问/接口暴露等网络攻击威胁。

1）近年来，由黑客渗透入侵导致的数据泄露事件增速越来越快，已经跃升为第一因素；

2）由于服务器配置不当、漏洞等因素造成的未授权访问问题也呈增速发展；

3）内部人员窃取或丢失数据造成的数据泄露问题，近几年来逐渐减少。

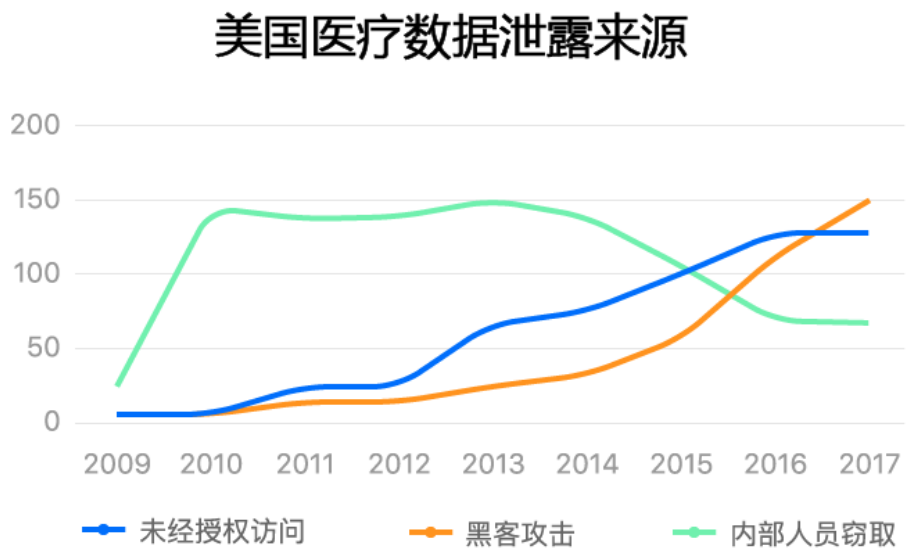


图 3_2_2：美国医疗数据泄露来源

3.1 线上医疗服务存在逻辑漏洞，可导致数据泄露

第三方医疗服务等线上医疗服务平台在为患者看病就诊带来便利的同时，也给攻击者提供了新的攻击入口，带来了更多的安全风险。

第三方医疗服务平台往往会在同一个平台或者同一个代码框架下，汇集众多医疗机构的资源，以便于为多家医院提供线上挂号预约、体检预约以及医生咨询等服务，一旦有平台出现严重的信息泄露等漏洞就会影响平台上所有医院。

另外囿于第三方医疗服务平台服务商对安全的重视程度及条件的限制，使得第三方医疗服务平台出现信息泄露等安全漏洞的几率增大。

腾讯智慧安全发现，国内多家三甲医院接入的第三方医疗服务平台存在严重逻辑漏洞，这些漏洞可导致平台就诊患者信息泄露，具体包括如下类型：

1）个人身份信息：姓名、手机号、身份证号、家庭住址、网络 ID。

2）就诊信息和医疗诊断数据：挂号记录、检查检验报告、住院记录、体检报告、缴费记录等。

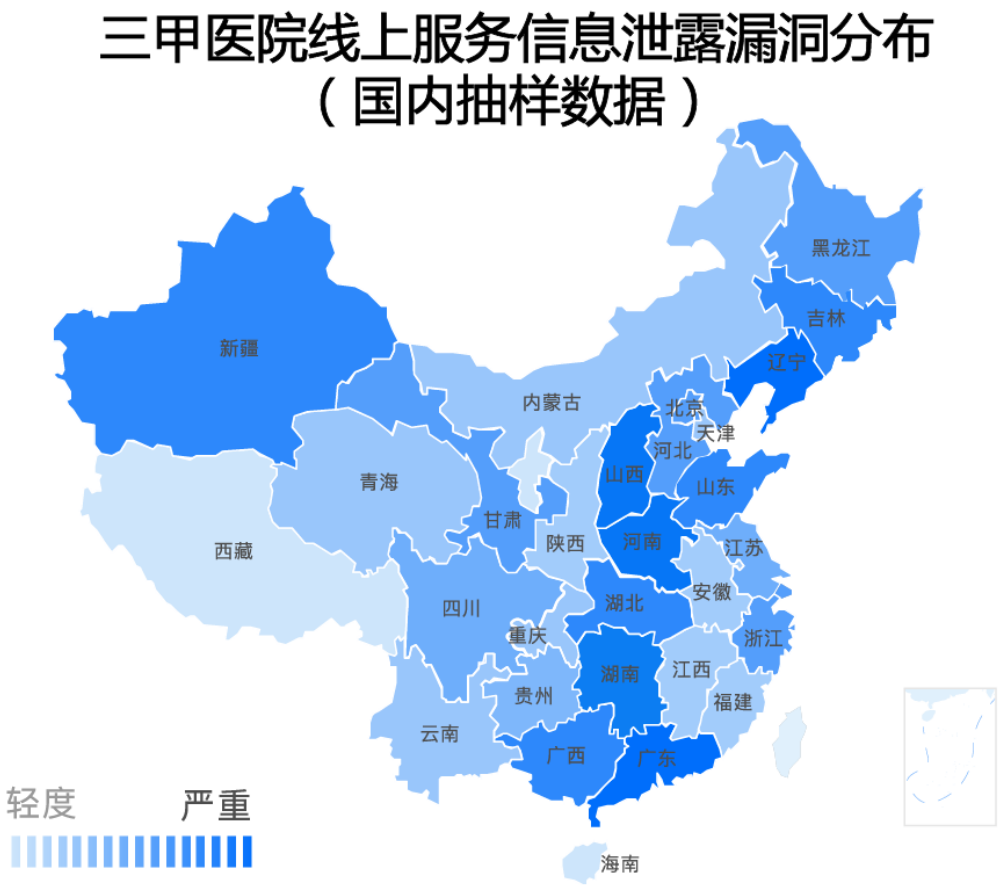


图 3_1_1　三甲医院线上服务信息泄露漏洞分布（国内抽样数据）

今年 7 月，安全团队在日常守护全网用户信息安全工作过程中，发现某健康医疗平台存在多个漏洞。包括登录绕过、未授权访问、平行越权等严重漏洞，攻击者仅通过手机号就可以获取到患者的姓名、身份证，就诊卡信息、挂号记录、化验检验报告单以及其他个人健康生理和医疗信息。

图 3_1_2　某第三方健康医疗平台越权访问演示图

根据腾讯智慧安全御见威胁情报中心分析发现，该第三方平台的数据泄露问题涉及到全国多个省市数百家大型三甲医院（如下图所示），大量患者的个

人身份信息和医疗就诊信息存在泄露风险，如果被黑客攻击、利用，则后果不堪设想。

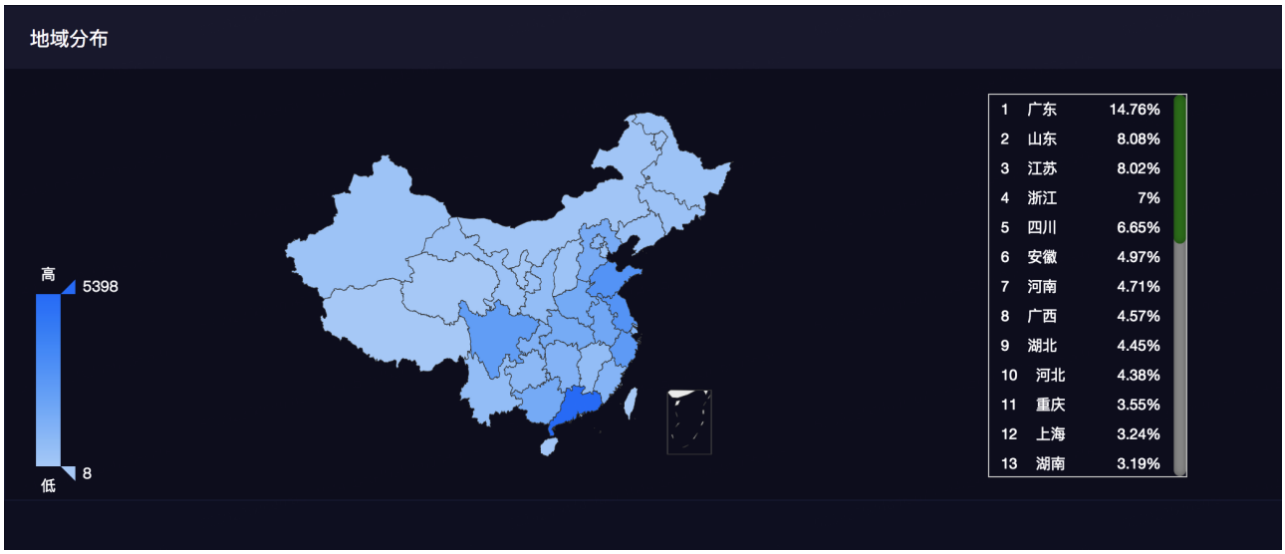


图 3_1_3　某第三方健康医疗平台数据泄露漏洞影响情况

在腾讯智慧安全的协助下该平台的漏洞已得到妥善修复。但此类问题普遍存在，应当引起重视。

3.2 大量敏感端口开放提供攻击入口

网络设备的敏感端口和服务直接暴露在互联网上，会降低黑客入侵以及未授权访问的技术门槛，从而增加数据泄露风险，或将导致严重的数据泄露危机。

基于对互联网资产的探测分析，腾讯智慧安全发现 71%的三甲医院存在高危端口开放情况，如下图所示。

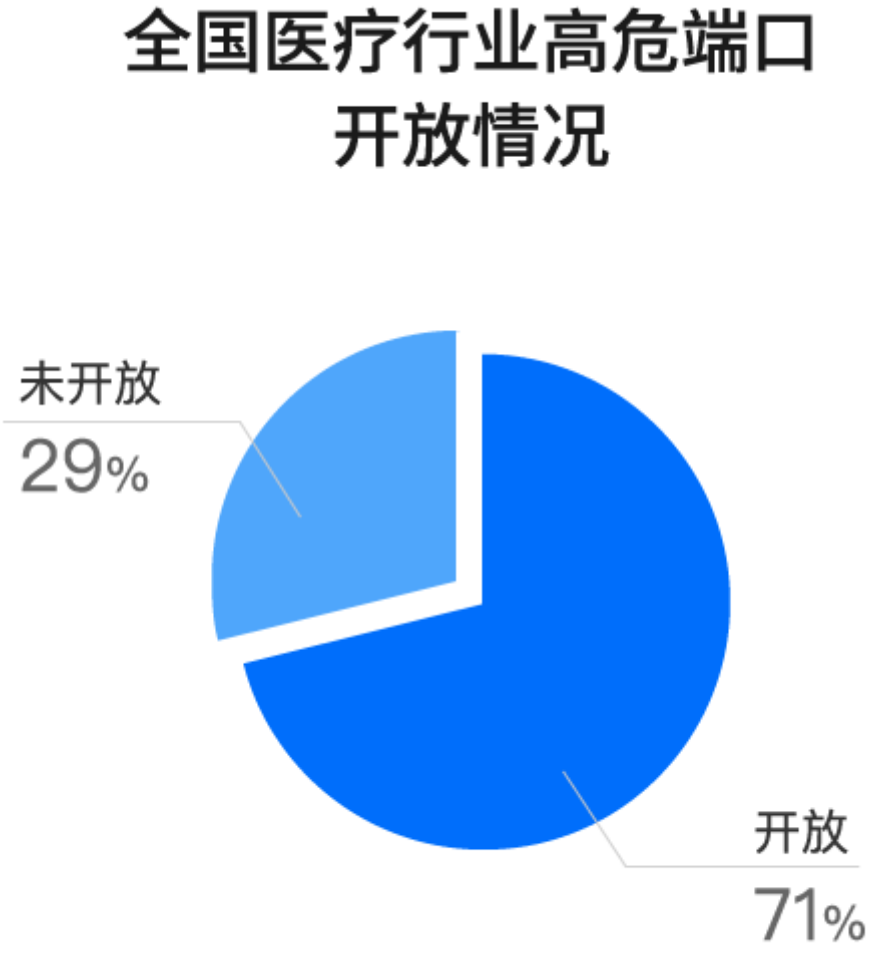


图 3_2_1　全国医疗行业高危端口开放情况

以最近几年黑客攻击事件中出现频率较高的高危端口为参照：

1）超过 1/3 的医院将 SSH 登录、MySQL 数据库服务等端口直接开放于外网，这些端口的开放，为黑客入侵医疗机构系统提供了便利。

2）值得一提的是，数据库系统的直接暴露还会增加勒索攻击的风险，危及医疗业务的连续性，数据库攻击者，除了窃取数据信息（拖库）之外，还可能针对数据库的数据实施经济勒索攻击。攻击者先将数据库进行备份，然后利用远程命令删除数据库从而实施勒索。

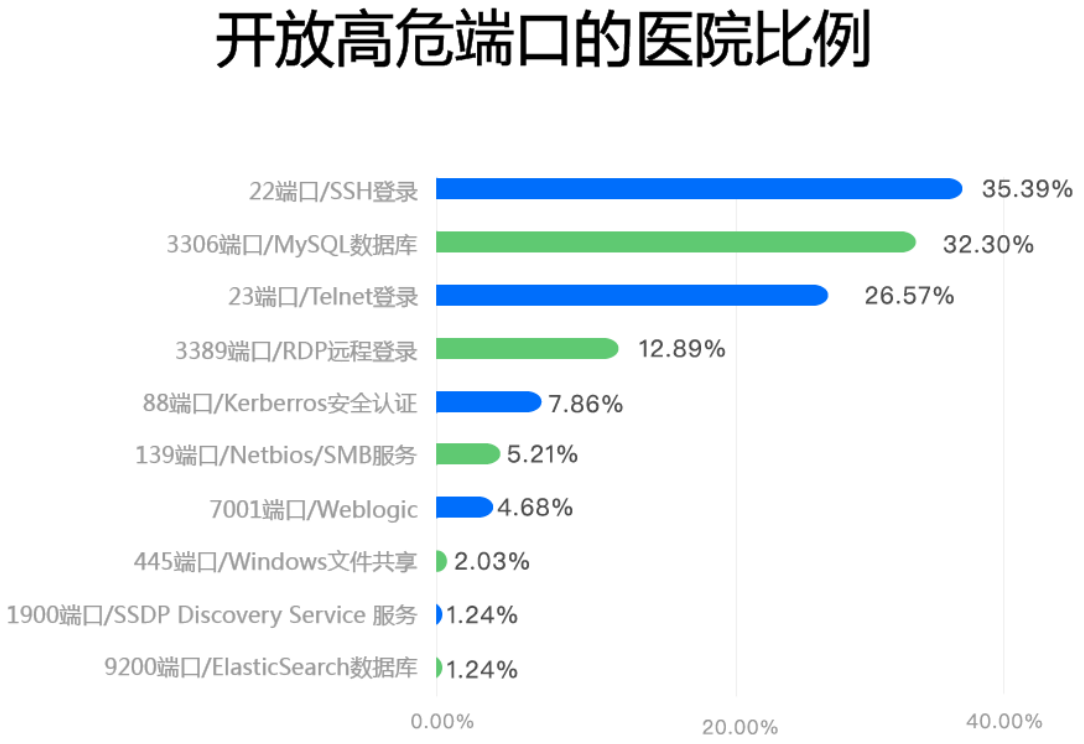


图 3_2_2　开放高危端口的医院比例

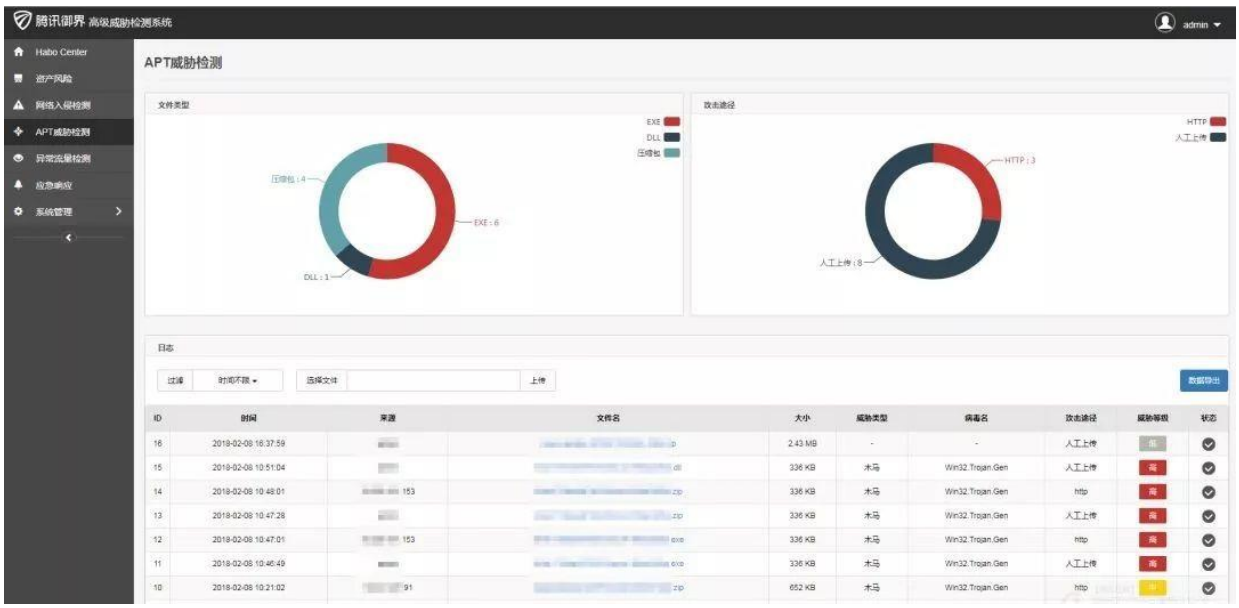
4、应对方案及建议

针对本报告中发现的安全问题及可能带来的业务安全风险，腾讯智慧安全建议相关医疗机构高度重视数据安全问题，切实保护广大患者的敏感信息，慎重存储和使用医疗敏感数据。同时加强在医疗信息安全领域的投入、建立系统化的安全保障体系，从事件的被动应急响应提升为安全风险的主动感知，从而提升安全管理能力。

1）首先针对已知的安全问题，对线上服务进行自查或由第三方安全机构进行协助排查修复；

）加强医疗服务平台的上游服务商或团队的要求和审核，保证相关服务的安全性和可靠性；

3）选择专业的医疗安全解决方案，建设安全防御体系，建议使用腾讯御界高级威胁检测系统。御界高级威胁检测系统，是基于腾讯反病毒实验室的安全能力、依托腾讯在云和端的海量数据，研发出的独特威胁情报和恶意检测模型系统。



建议全网安装御点终端安全管理系统。御点终端安全管理系统具备终端杀毒统一管控、修复漏洞统一管控，以及策略管控等全方位的安全管理功能，可帮助企业管理者全面了解、管理企业内网安全状况、保护企业安全。

4）建立面向行业的应急响应协同机制，及时预警联防共治，携手应对网络安全风险。