https://www.qianxin.com

奇安信
新一代网络安全领军者

95015
网络安全服务热线

2022

医疗卫生行业网络安全分析报告

THE REPORT

发布机构：

奇安信行业安全研究中心
补天漏洞响应平台
奇安信安全托管团队
奇安信安服团队
安全内参

主要观点

◎ 医疗卫生行业网络安全建设水平在近年来得到了快速提升。以补天平台收录的医疗卫生行业网站漏洞为例，网站漏洞修复率高达 98.9%，显著高于平均水平 97.8%，在所有行业中排名居前。同时，针对行业应急响应事件的分析也显示，96.4% 的事件是医疗卫生行业机构自主发现的，这一水平也较前些年有显著提升。

◎ 弱口令问题仍是困扰医疗卫生行业网络安全建设的痛点和难点。行业网站漏洞中，弱口令占有 13.4%；在运营风险事件中，弱口令事件占 30.0%。同时，弱口令问题也是网络安全应急响应事件重要诱因。

◎ 数据安全已经成为医疗卫生行业网络安全建设不容忽视的重要一环。例如，在行业网站漏洞中，信息泄露漏洞占 21.7%；在运营风险事件中，信息泄露事件占 12.6%；在行业网络安全应急响应事件中，有 7.1% 的攻击者是为了窃取重要数据，最终导致数据丢失和数据被篡改等损失的事件占到了所有应急响应事件的近四成。

◎ 恶意程序和漏洞利用是医疗卫生行业面临的最主要的网络安全风险。这两种类型风险在所有运营风险事件中占比 95.7%，在网络安全应急响应事件中占比 76.2%，是攻击者最为青睐的攻击手段。一旦攻击成功，将会造成不可估量的损失，甚至威胁患者的生命安全：2021 年，在美国就出现了首例因勒索软件攻击直接导致个人死亡的网络安全事件。

◎ 信息化设备的日常规范使用和管理应当引起医疗卫生行业的高度重视。在行业网络安全应急响应事件中，有 16.7% 并不是由网络攻击事件触发，而是由于机构内部运营故障、操作失误或管理疏失所造成的。这也表明，网络安全工作与业务运营密不可分的。文中第四章第二节，就是鲜活典型案例。

摘 要

◎ 2021 年全年，补天漏洞响应平台共收录全国医疗卫生行业相关网站的安全漏洞 2568 个，占全年各类网站安全漏洞的 1.8%。

◎ 医疗卫生行业网站漏洞中，通用型漏洞占比 0.3%，事件型漏洞占比 99.7%。

◎ 从网站的 IP 归属地（省级）来看 , 来自北京市的医疗卫生行业网站被报告漏洞数量最多，占比约为 12.7%；其次是青海省，占比为 9.4%；广东省排第三，占比 9.1%。

◎ 医疗卫生行业网站漏洞中，高危漏洞占比 38.4%；中危漏洞占比 52.7%；低危漏洞占比 8.9%。

◎ 医疗卫生行业网站漏洞中，信息泄露漏洞占比最高，达 21.7%，其次是命令执行漏洞，占比 21.0%，弱口令占比 13.4%。

◎ 相较于夜间（20：00~08：00），医院在日间（08：00~20：00）更容易遭受网络攻击，日间发生的风险事件占风险事件总数的 79.1%。

◎ 从一周情况来看 , 周四是一周中医疗卫生行业风险事件最为高发的一天，占比为 22.2%，其次在周五和周一，分别占比 18.9% 和 17.7%。

◎ 从医疗卫生行业风险事件持续时长来看，攻击时长持续不到一分钟的事件占比 44.6%，其中时长在 1 秒以内的占总量的 39.1%。

◎ 医疗卫生行业风险事件以漏洞利用和恶意程序为主。漏洞利用占比 66.0%，恶意程序占比 29.7%。，其他类型占比 4.3%。

◎ 在医疗卫生行业漏洞利用类型的风险事件中，弱口令漏洞占比最高，达 47.8%，信

◎ 息泄露漏洞占比 12.6%，后门漏洞占比 11.9%，未授权访问漏洞占比 10.1%，暴力破解漏洞占比 5.7%。

◎ 在医疗卫生行业恶意程序类型的风险事件中，远控木马类型占比 41.0%，挖矿木马类型占比 24.1%，勒索病毒类型占比 12.0%。

◎ 2021 年全年，奇安信安服团队共参与处置医疗卫生行业网络安全应急响应事件 84 起。其中，相关机构自行发现的网络安全事件占 96.4%，16.7% 是通过内部安全运营巡检的方式自主查出，79.7% 是因为其网络系统已经出现了显著的入侵迹象，或者已遭到了攻击者的敲诈勒索。由监管机构、主管单位、第三方平台通报处置的网络安全事件占 3.6%。

◎ 医疗卫生行业网络安全应急响应事件的影响范围中，业务专网设备占比 81.0%，互联网设备占比 19.0%。

◎ 从医疗卫生行业网络安全应急响应事件的攻击者意图来看，敲诈勒索和黑产活动占比最高，占比分别为 51.2% 和 25.0%。同时，有 7.1% 是为了窃取重要数据，还有 3.6% 属于内部违规。

◎ 对 2021 年医疗卫生行业安全事件攻击类型进行分析，排名前三的类型分别是：恶意程序占比 46.4%；漏洞利用占比 29.8%；钓鱼邮件占比 3.6%。在恶意程序中，木马攻击（非蠕虫病毒）占比 51.3%，蠕虫病毒攻击占比 48.7%。

◎ 在 2021 年的医疗卫生行业的网络安全应急响应事件中，有 16.7% 并非是由网络攻击事件触发的。

◎ 从医疗卫生行业被攻陷系统的损失来看，数据丢失占比最高，达 29.8%；其次是系统 / 网络不可用，占比 16.7%；生产效率低下排第三，占比 11.9%。

关键词：医疗卫生行业、安全漏洞、风险事件、应急响应

目录

CONTENTS

研究背景

2019 年 12 月以来，新型冠状病毒感染肺炎疫情在全国蔓延。国家卫生健康委员会为贯彻落实党中央、国务院关于新型冠状病毒感染的肺炎疫情防控工作的总体部署，充分发挥信息化在辅助疫情研判、创新诊疗模式、提升服务效率等方面的支撑作用，在总结各地典型做法的基础上，制定出台了《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》国卫办规划函〔2020〕100 号，要求“加强网络信息安全工作，以防攻击、防病毒、防篡改、防瘫痪、防泄密为重点，畅通信息收集发布渠道，保障数据规范使用，切实保护个人隐私安全，防范网络安全突发事件，为疫情防控工作提供可靠支撑。”随着我国新型冠状病毒感染肺炎疫情逐步得到控制，社会对医疗卫生行业的信息化建设所起到的成效有目共睹，同时也暴露出我国医疗体系中的一些短板。

“十三五”将医疗卫生信息化纳入其中作为网络安全和信息化建设的重点。2020 年 3 月 5 日，《中共中央国务院关于深化医疗保障制度改革的意见》（以下简称《意见》）发布，提出我国未来 5 年—10 年医疗改革的目标和任务。医疗信息化建设有望提速，《意见》出台的新意在于“高起点推进标准化和信息化建设”和“建立管用高效的医保支付机制”。《意见》提出，高起点推进标准化和信息化建设。统一医疗保障业务标准和技术标准，建立全国统一、高效、兼容、便捷、安全的医疗保障信息系统，实现全国医疗保障信息互联互通，加强数据有序共享。

随着疫情防控的需要、信息化的不断发展与国内居民在自身健康需求关注度的逐渐提升，医疗卫生行业为了提升我国居民医疗健康的管理与服务水平，通过信息化手段例如远程诊疗、移动诊疗、医疗物联网的方式拓展了各类医疗信息化的应用场景，互联网医院的开展也改变了传统线下就诊的服务模式，云计算、大数据的不断深化应用也让医疗信息化不再受传统 IT 服务架构的桎梏，医疗数据的

价值进一步得到提升。但是，在这背后也存在着亟待解决的一些安全风险与问题。

为了深入了解医疗卫生行业网络安全建设水平与运营现状，为医疗卫生行业各单位提升网络安全实战化保障能力提供参考依据，奇安信行业安全研究中心与医疗卫生行业一线运营团队联合编撰了《2022 医疗卫生行业网络安全分析报告》。

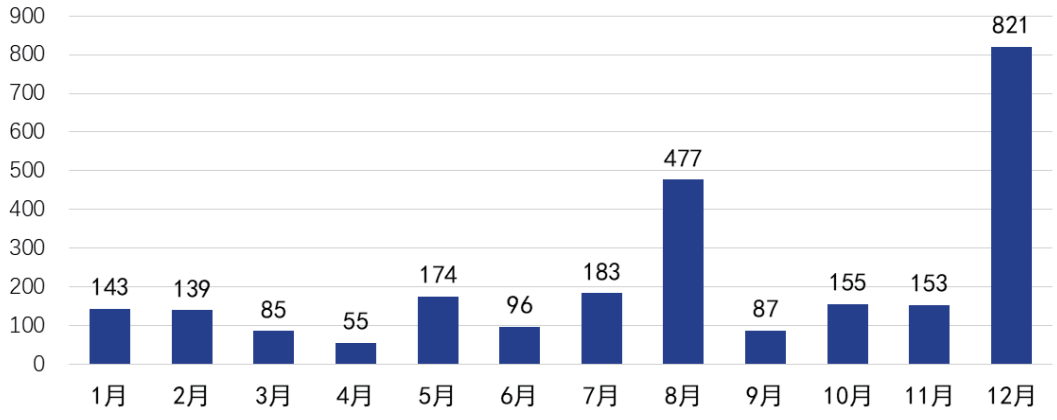
报告从安全漏洞、运营风险、应急响应等多个维度出发，通过数据、案例等多种方式对医疗卫生行业网络安全现状展开全面分析。报告内容涉及医疗卫省行业网站 2100 个，应急响应事件 84 起，及百余起医疗卫生行业网络安全运营风险事件。

第一章
医疗卫生行业安全漏洞分析

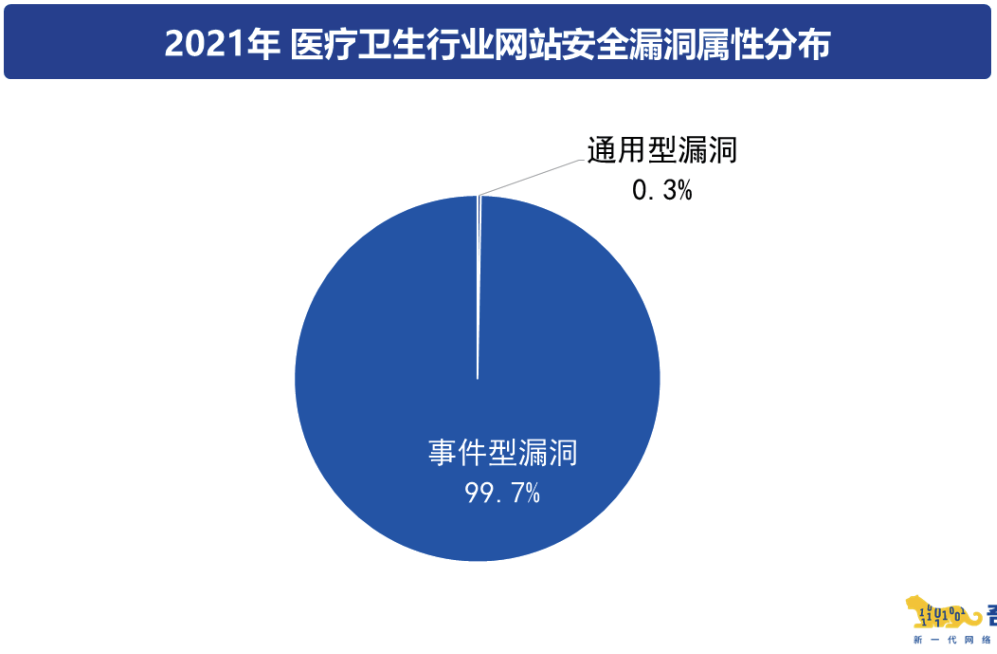
网站是政府和企业重要的信息化平台。网站安全也是政企机构最为关注的网络安全问题之一。近年来，国内大中型政企机构的网站安全建设已然取得了巨大的进步，但安全隐患仍然普遍存在。

2021 年 1-12 月，补天漏洞响应平台（以下简称：补天平台）共收录全国医疗卫生行业相关网站的安全漏洞 2568 个，占全年各类网站安全漏洞的 1.8%，涉及国内医疗卫生行业网站 2100 个。其中，12 月份收录的漏洞数量最多，为 821 个。

2021年 补天平台每月收录医疗卫生行业网站漏洞个数



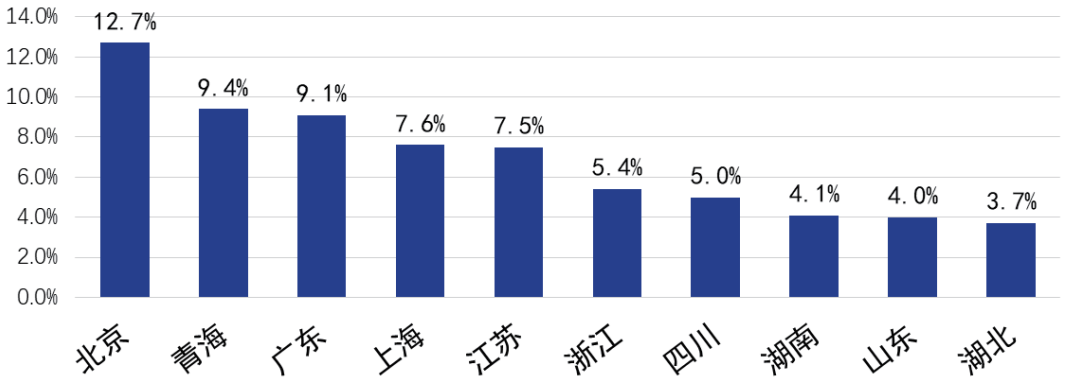
从漏洞属性分布来看，2021 年全年补天平台收录的医疗卫生行业相关网站的安全漏洞中，通用型漏洞占比 0.3%，事件型漏洞占比 99.7%。



其中，通用型漏洞是指某一类系统共同存在的安全漏洞，具有一定的普适性，通常可以通过标准化方法进行检测。而事件型漏洞则是指某一个系统特有的安全漏洞，一般与系统的管理、配置不当或特殊开发过程等因素有关，一般需要通过人工挖掘来发现。

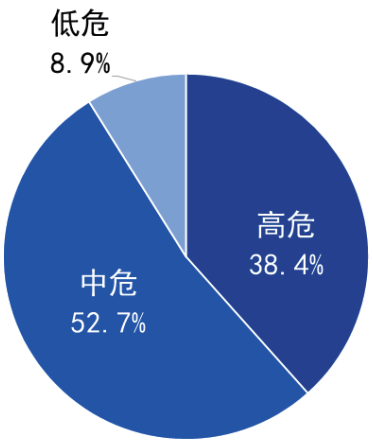
从网站的 IP 归属地（省级）来看，来自北京市的医疗卫生行业网站被报告漏洞数量最多，占比约为 12.7%；其次是青海省，占比为 9.4%；广东省排第三，占比 9.1%。

2021年 医疗卫生行业网站漏洞数量省级行政区分布TOP10



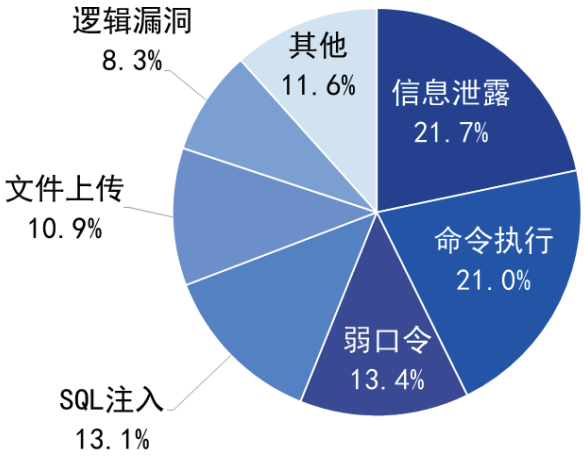
从漏洞的危险等级来看，高危漏洞占比为 38.4%；中危漏洞占比为 52.7%；低危漏洞占比为 8.9%。

2021年 医疗卫生行业网站安全漏洞等级分布



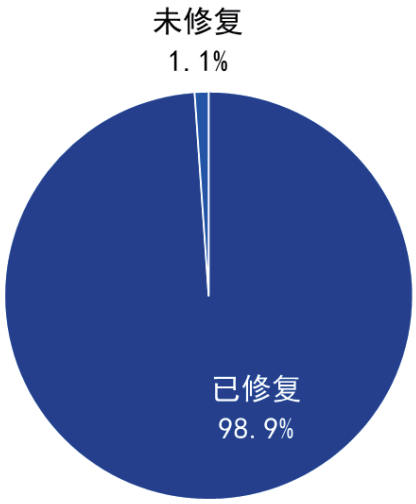
从漏洞的技术类型来看，信息泄露漏洞最多，占比为 21.7%，其次是命令执行漏洞，占比为 21.0%，弱口令漏洞，占比为 13.4%。具体漏洞类型分布请见下图。

2021年 医疗卫生行业网站安全漏洞类型分布



2021 年全年，在补天平台收录的医疗卫生行业网站漏洞中，98.9% 网站漏洞已经进行了修复，1.1% 的网站漏洞未进行修复。这一修复比例，远高于补天平台平均漏洞修复率 97.8%，在所有行业中，排名居前。

2021年 补天平台收录医疗卫生行业网站漏洞修复情况



第二章
安全运营风险事件特征分析

一、安全运营风险事件

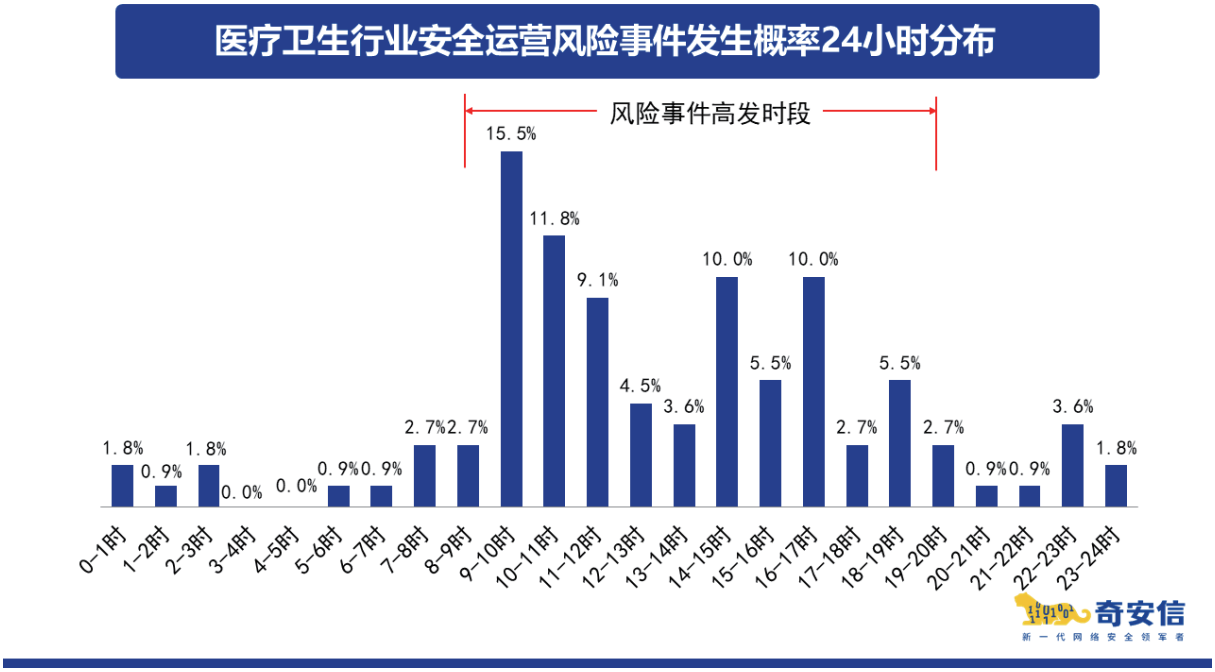
安全运营风险事件（以下简称“风险事件”）是指网络用户由于计算机系统或设备相关因素、用户自身安全意识薄弱或者遭到外部攻击入侵导致的，在网络使用过程中存在一定风险，容易造成用户损失的网络安全事件。

奇安信安全托管服务通过采集安全设备产生的网络流量、网络日志、安全日志、主机日志等数据信息，结合威胁预警情报分析发现客户侧的数据失窃密、非法连接与控制、系统破坏等行为，集合威胁情报库等信息，判定攻击来源组织、攻击工具、攻击技术、战术目标等，深度发现潜在的攻击行为和控制通道，为客户本地侧检测发现、追踪溯源、应急响应等提供技术支撑。本章内容基于奇安信安全托管服务团队数据，对 2022 年以来监测到的 100 余起典型风险事件进行了综合分析。

二、风险事件发生时间

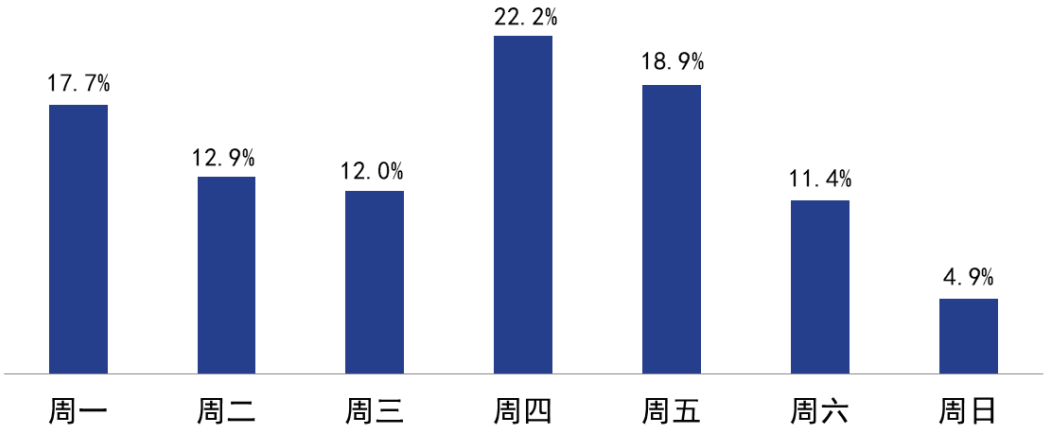
下图给出了风险事件发生时间在 1 天 24 小时内的分布情况，统计显示，

09：00~10：00 是风险事件最为高发的时段，在全天占比高达 15.5%，其次是 10：00~11：00，风险事件的发生率占全天的 11.8%。此外，在 14：00~15：00 和 16：00~17：00 也是风险事件高发时段。总体来看，相较于夜间（20：00~08：00），医院在日间（08：00~20：00）更容易遭受网络攻击，日间发生的风险事件占风险事件总数的 79.1%。分析认为，日间是医院业务最为繁忙的时间，接入网络和运行的各类设备、系统也最多，因此也更容易遭受各种各样的网络攻击。



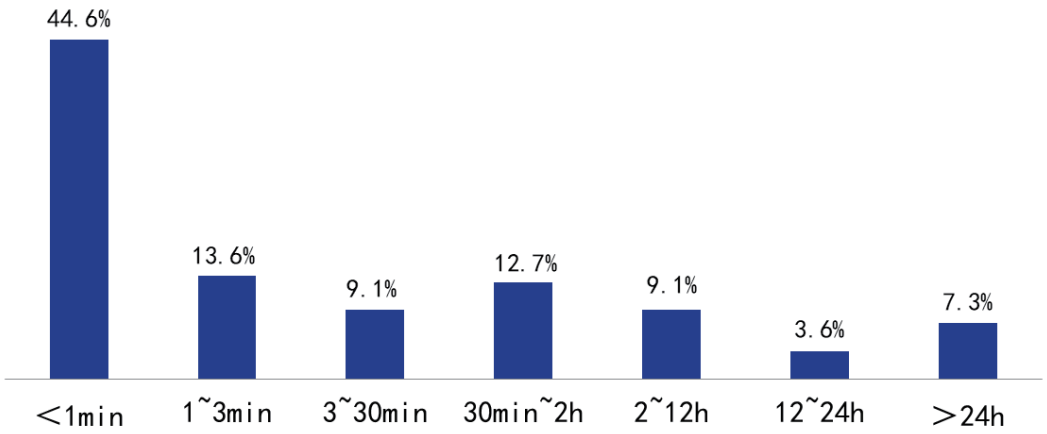
从一周情况来看，周四是一周中医疗卫生行业风险事件最为高发的一天，占比为 22.2%，其次在周五和周一，分别占比 18.9% 和 17.7%。医疗卫生行业一周七天风险事件发生概率分布如下图。

医疗卫生行业安全运营风险事件发生概率一周七天分布



从风险事件持续时长来看，攻击时长持续不到一分钟的事件占比 44.6%，其中时长在 1 秒以内的占总量的 39.1%。攻击时长在 1~3 分钟的事件占比 13.6%，3~30 分钟的事件占比 9.1%。医疗卫生及行业风险事件持续时长分布如下图。

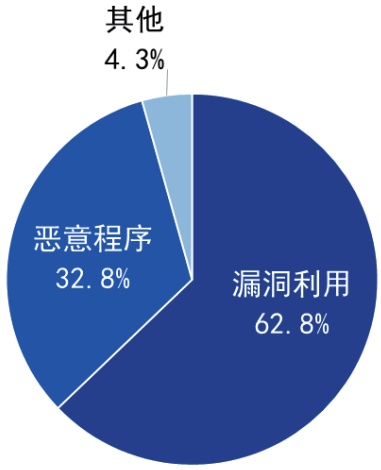
医疗卫生行业风险事件持续时间分布



三、风险事件攻击手法

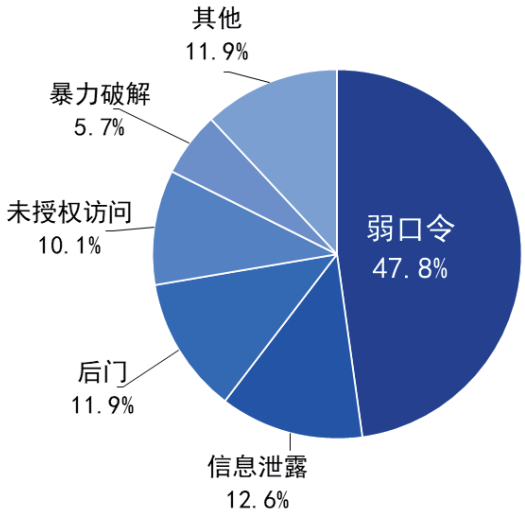
从攻击手法来看，医疗卫生行业风险事件以漏洞利用和恶意程序为主。漏洞利用占比 66.0%，恶意程序占比 29.7%。，其他类型占比 4.3%。

医疗卫生行业风险事件攻击手法分析



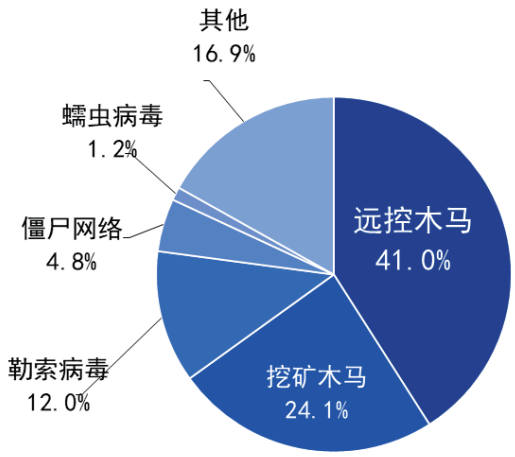
漏洞利用类型的风险事件中，弱口令漏洞占比最高，达 47.8%，信息泄露漏洞占比 12.6%，后门漏洞占比 11.9%，未授权访问漏洞占比 10.1%，暴力破解漏洞占比 5.7%。弱口令依然是医疗卫生行业应该引起高度重视的安全问题。

医疗卫生行业风险事件中漏洞利用类型分布



恶意程序类型的风险事件中，远控木马类型占比 41.0%，挖矿木马类型占比 24.1%，勒索病毒类型占比 12.0%。具体恶意程序类型分布如下图。

医疗卫生行业风险事件中恶意程序类型分布



远控木马可以让攻击者完全控制被成功入侵的计算机设备，可以利用它完成一些甚至连用户都不能顺利进行的操作。由于要达到远程控制的目的，该种类的木马往往集成了其他功能，使得攻击者可以在计算机上为所欲为，例如可以任意访问、删除、拷贝文件等，可能使得医疗卫生行业许多敏感数据被泄露。

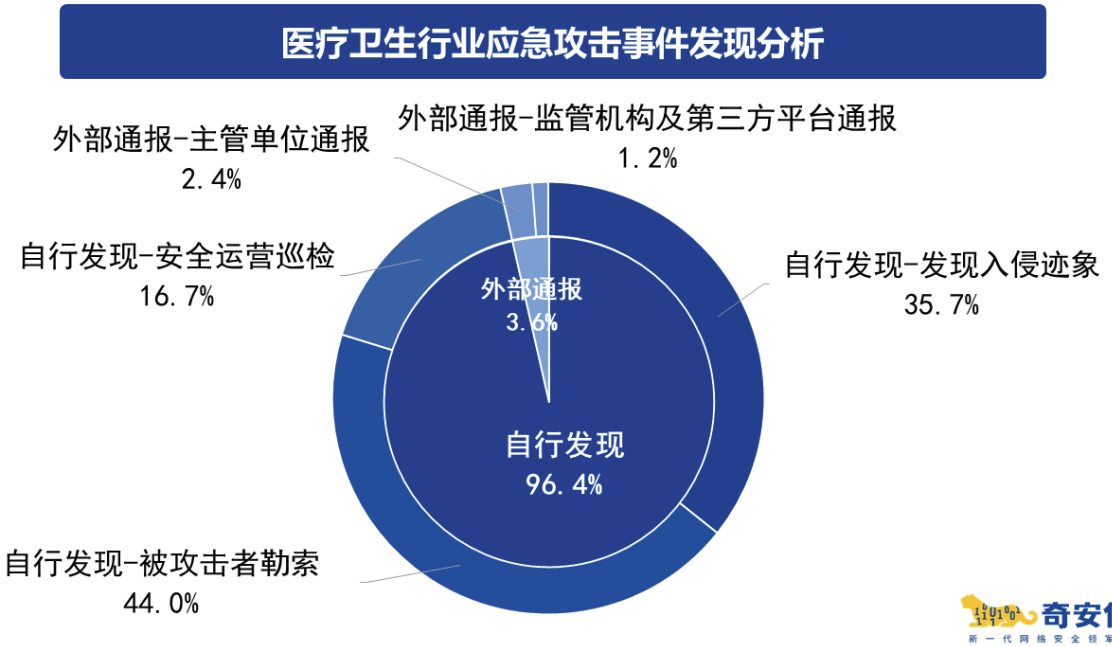
挖矿木马是指攻击者通过各种手段将挖矿程序植入受害者的计算机中，在用户不知情的情况下，利用受害者计算机的运算力进行挖矿，会导致用户系统资源被恶意占用和消耗、硬件寿命被缩短，会严重影响医疗卫生行业的业务运行。

除此之外，勒索病毒、僵尸网络等都是攻击者青睐的恶意程序类型的攻击手段。更有甚者，在一次风险事件中，攻击者会使用包括漏洞利用和恶意程序类型的多种手段对医疗卫生行业的网络系统进行攻击，如果不能及时监测和处置，可能会造成不可估量的业务损失，甚至会危及患者的生命。

第三章
医疗卫生行业应急响应形势分析

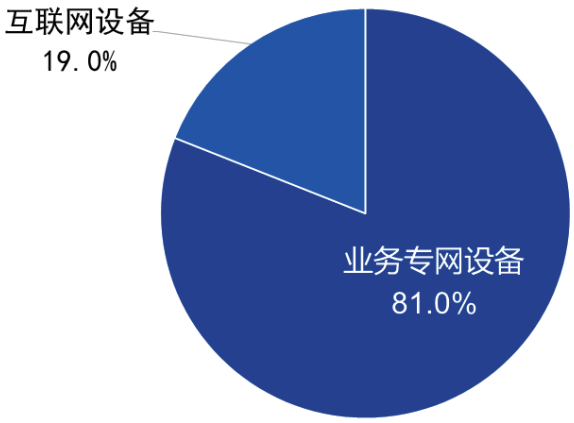
2021 年 1-12 月，奇安信集团安服团队共参与和处置全国范围内医疗卫生行业网络安全应急响应事件 84 起，第一时间协助用户处理安全事件，确保了用户门户网站、数据库、办公系统和重要业务系统的持续安全稳定运行。

在奇安信集团安服团队参与处置的医疗卫生行业网络安全应急响应事件中，相关机构自行发现的网络安全事件占 96.4%，其中 16.7% 通过内部安全运营巡检的方式自主查出，79.7% 是因为其网络系统已经出现了显著的入侵迹象，或者已遭到了攻击者的敲诈勒索。由监管机构、主管单位、第三方平台通报处置的网络安全事件占 3.6%。



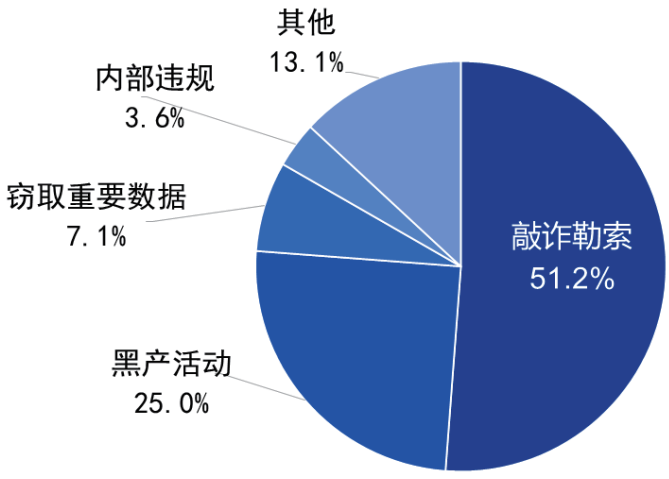
医疗卫生行业网络安全应急响应事件的影响范围中，业务专网设备占比81.0%，互联网设备占比19.0%。下图为医疗卫生行业网络安全应急响应事件影响范围分布。

医疗卫生行业网络安全应急响应事件影响范围分布

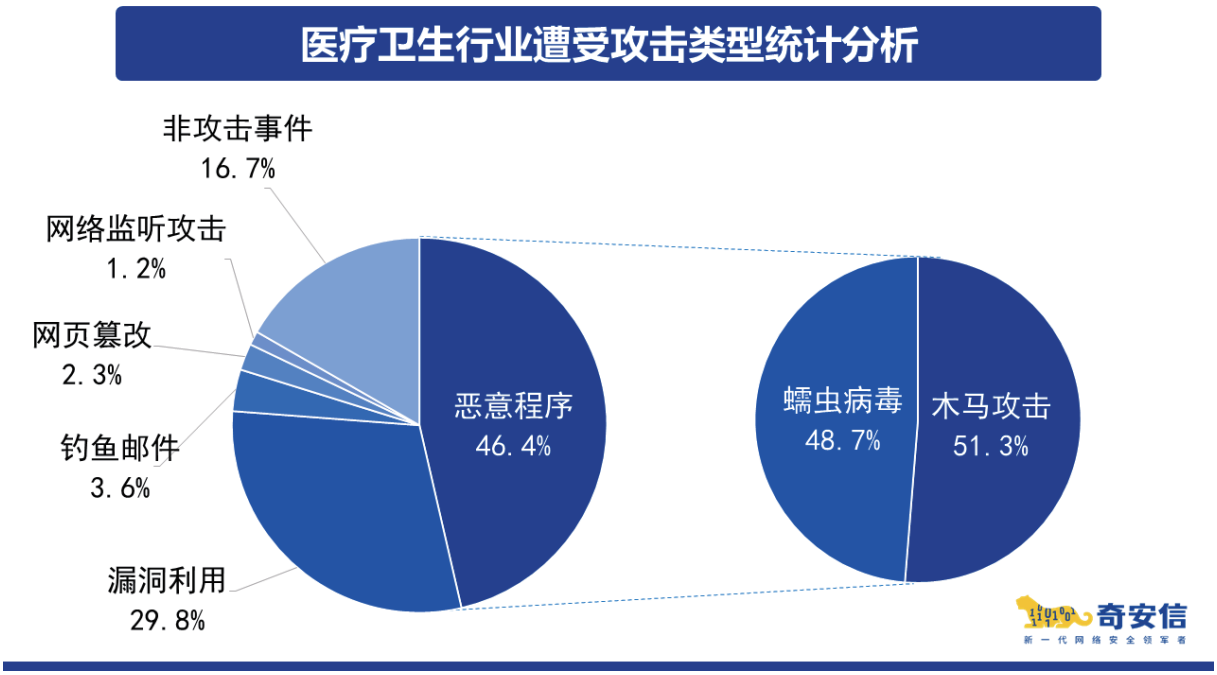


从攻击者意图来看，敲诈勒索和黑产活动占比最高，占比分别为51.2%和25.0%。同时，有7.1%是为了窃取重要数据，还有3.6%属于内部违规。

攻击者针对医疗卫生行业的攻击意图排行



通过对 2021 年医疗卫生行业安全事件攻击类型进行分析，排名前三的类型分别是：恶意程序占比 46.4%；漏洞利用占比 29.8%；钓鱼邮件占比 3.6%。在恶意程序中，木马攻击（非蠕虫病毒）占比 51.3%，蠕虫病毒攻击占比 48.7%。



蠕虫病毒、木马由于传播速度快、感染性强等特征成为最受攻击者青睐的攻击手段，攻击者利用病毒、木马对办公系统进行攻击，通常会产生大范围感染，造成系统不可用、数据损坏或丢失等现象；例如 11 月出现的“Magniber 勒索病毒”对服务器和系统进行攻击，导致系统不可用，从而谋取利益。

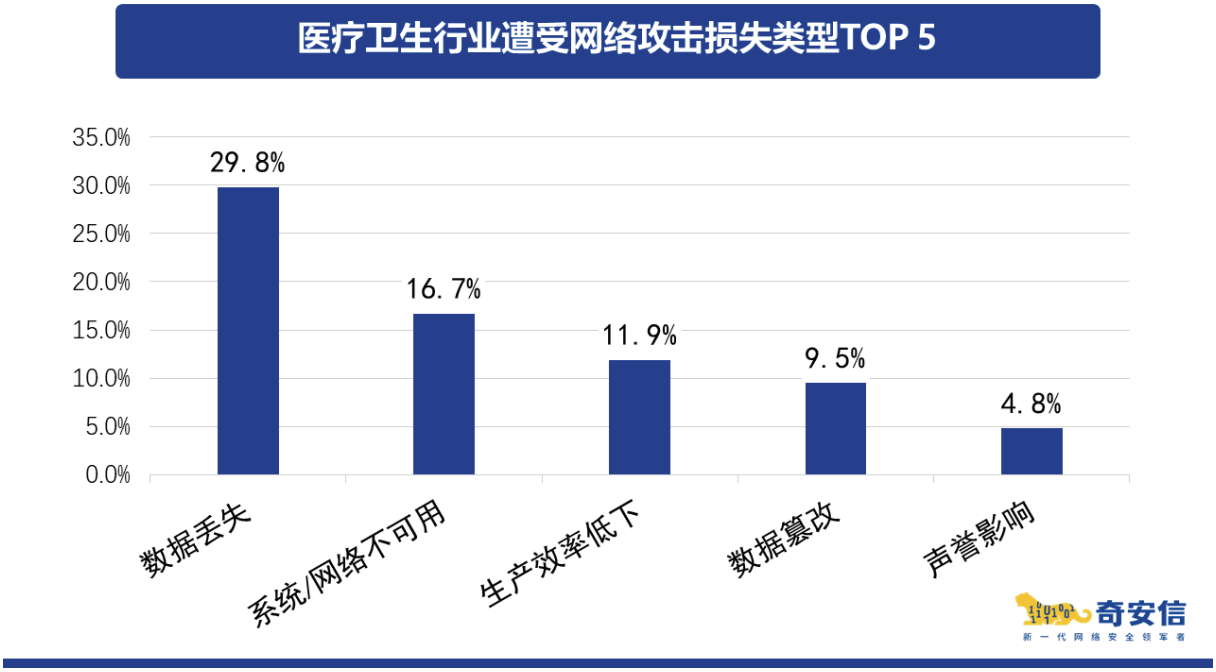
漏洞利用则是攻击者利用政企机构网络安全建设不完善的弊端，使用常见系统漏洞、Web 漏洞等发起攻击。例如 2021 年 12 月发现的“Apache Log4j2 漏洞”，就被大量攻击者利用对服务器进行的破坏性攻击，通常会导致重要数据丢失、泄露、内部投毒、敲诈勒索等严重后果。

除此之外，钓鱼邮件、网页篡改、网络监听攻击等也是较为常见的攻击类型。如 2021 年 12 月份发现的 emote 木马钓鱼邮件，一旦中招，对政企机构产生的

影响是不小的。医疗卫生行业机构应做好员工安全意识培训工作，定期内部巡检，及时发现威胁并有效遏制。

特别值得注意的是，在 2021 年的医疗卫生行业的网络安全应急响应事件中，还有 16.7% 并非是由网络攻击事件触发的。这些事件绝大多数都是机构内部运营故障、操作失误或管理疏失所造成的。这也提醒我们，网络安全工作与业务运营是密不可分的。网络安全问题会影响业务开展，而业务问题也同样会触发网络安全事件。

从被攻陷系统的损失来看，数据丢失占比最高，达 29.8%；其次是系统 / 网络不可用，占比 16.7%；生产效率低下排第三，占比 11.9%。具体分布如下所示。



第四章
医疗卫生行业应急响应典型案例

一、某三甲医院部分内网设备被勒索加密

（一）场景回顾

2021 年 10 月，某地一家三甲医院门诊部内部系统无法正常使用，信息科工作人员检查发现部分服务器上文件被加密，故请求安服团队支持进行分析处置。

（二）事件分析

现场分析处置过程中发现，除了被报告的几台服务器设备外，还有多台服务器和医用终端被勒索病毒加密，应用无法使用，数据被加密。通过溯源分析发现，攻击者通过服务器远程桌面口令爆破登录到服务器后，以服务器作为跳板接入内网，之后对其他服务器和医用终端进行了远程桌面口令撞库，获取了一台具有双网卡的服务器权限，并对内网发起大规模撞库，获取大量服务器权限，并通过跳板机以人工方式进行投毒。

（三）处置方案

1）切断网络，阻断攻击者连接，同时对重要信息系统 PACS 进行业务恢复；

2）在服务器和终端上逐一安装杀毒和安全防护软件，修复系统漏洞，更新病毒库；

3）修改所有服务器、医用终端密码，重要信息系统使用不同密码，保证密码复杂度并定期进行更改，杜绝使用弱口令。

二、某三级综合医院部分电脑 C 盘文件无端被删

（一）场景回顾

2021 年 9 月，某地一家三级综合性医院部分电脑存在卡顿黑屏现象，C 盘大量文件被删。医院工作人员怀疑电脑疑似感染挖矿木马。

（二）事件分析

应急人员在现场首先对某一问题机器进行排查分析，发现存在可疑恶意进程和敏感端口开放情况，并且系统用户也存在使用弱口令等问题，但这些问题并非是导致电脑卡顿、黑屏和 C 盘文件被删的主要原因。

应急人员使用专杀工具对问题电脑进行病毒查杀，发现某个会造成系统黑屏和卡顿的病毒文件。但病毒程序并不会破坏或删除 C 盘文件。

进一步排查发现，电脑的打印程序存在某个配置，不仅会造成系统卡死，还会导致系统重启后大部分文件被删除。在与医院的 IT 运维人员沟通后确认，医院使用的医用仪器检验管理系统日前新增了一个配置策略，该策略会使电脑在打印包含图片的病例时，会先检查 C 盘空间是否充足，若不充足会删除自建的临时文件。但由于软件运维人员在配置该系统时，误把“C:\”目录添加到了删除目录中，造

成系统在打印某些病例时会把 C 盘根目录所有文件删除。

（三）处置方案

1) 修改不当的系统配置，排查其他可能有风险的设备；

2) 排查发现系统存在空口令、弱口令和敏感端口开放的设备，要求增强口令强度，关闭不必要端口，或配置特定端口仅对特定 IP 地址开放；

3) 安装相应的防病毒软件，及时对病毒库进行更新，并且定期进行全面扫描，加强服务器上的病毒清除能力。

三、某专科医院内网大规模感染蠕虫病毒

（一）场景回顾

2021 年 4 月，某地一家专科医院内网 200 余台主机感染蠕虫病毒，杀毒软件查杀后仍会出现病毒，部分异常程序无法清除，干扰正常业务应用使用，部分终端无法部署新的业务系统。

（二）事件分析

应急人员现场对一台感染病毒的主机进行病毒定性分析，使用奇安信天擎对病毒进行查杀，初步判断为蠕虫病毒，并发现存在仿冒系统进程的异常程序，异常程序存在守护进程和自启动选项。

随后，应急人员又对某科室八台终端进行同样的排查，均发现启动项目录下

存在恶意程序，判断该恶意程序为操作系统感染所致。由于现场条件不允许进行情景再现模拟测试，故无法最终确定感染方式和时间。

（三）处置方案

1) 因装机方式特殊，且感染终端数量较多，因此没有采取逐台设备清除病毒的方法，而是对所有已经感染的终端重装了操作系统；

2) 部署高级威胁监测设备（如：奇安信天眼），及时发现恶意网络流量，同时可进一步加强追踪溯源能力，在安全事件发生时可提供可靠的追溯依据；

3) 建议医院上新业务和上新终端时，要对上新业务和终端进行安全检查或安全评估，检查和评估结果为安全后，再接入生产网络中去。

四、某三甲医院内网爆发永恒之蓝病毒

（一）场景回顾

2021 年 1 月，某地一家三甲医院内网十几台未安装安全软件的终端出现持续重启现象，疑似出现内网病毒，故请求奇安信安服团队协助检测最先感染病毒的终端并提供病毒信息，确认是否与外部网络攻击有联系。

（二）事件分析

应急人员现场对内网终端系统日志、流量威胁检测记录等进行取证分析，确认导致此次事件的直接原因是与永恒之蓝漏洞相关病毒。

应急人员在日志中发现相关漏洞利用痕迹，早在 2019 年 9 月就已经存在，故判定病毒存在一定的潜伏期。排查中还发现该医院对外服务器存在 Weblogic 反序列化命令执行严重漏洞，该漏洞可导致未授权用户通过远程服务器执行任意指令，但是该服务器与最先中毒的终端间未发现通信过程，故可排除外部直接、主动攻击的可能。病毒源的引入可能为点击恶意链接、浏览不良网页、插入了带病毒的 U 盘等。

（三）处置方案

1) 断开感染病毒终端的内网连接，对所有感染病毒的终端安装安全软件（如：奇安信天擎）并进行全盘杀毒；

2) 对 SMB 端口做合理限制，关闭所有不需要使用 445 端口的设备的 445 端口。并且关闭 IPC 的不安全共享，对所有内网终端进行 SMB 补丁安装，对外网服务器进行安全加固；

3) 部署高级威胁监测设备（如：奇安信天眼），及时发现恶意网络流量，进一步加强追踪溯源能力，在安全事件发生时可提供可靠的追溯依据。

五、某三甲医院内网服务器感染勒索病毒

（一）场景回顾

2021 年 10 月，某地一家三甲医院业务系统不可用，系统文件被加密勒索，故请求奇安信安服团队进行应急处置，分析病毒攻击行为。

（二）事件分析

现场对内网服务器进行排查，发现大量主机存在弱口令，如 1qaz2WSX、P@ssw0rd 等。此类口令虽然看似复杂，但是实际上属于常见键盘组合或常见字符替换，均属于流行弱口令库中排名靠前的口令，对于有经验的黑客来说并不难破解。

通过进一步的日志分析发现，多台服务器上都存在大量弱口令爆破行为，在过去几个月中，不止一路黑客曾经通过弱口令登录远程桌面进入医院服务器。而最后一个通过弱口令登入的攻击者，对服务器进行了勒索加密，根据被加密的文件名后缀判断，病毒为 LOCKBIT 勒索病毒，目前无法解密。

总体来看，该医院服务器长期使用弱口令，长期处于不安全状态，并曾遭多路黑客频繁攻击，发生重大安全事故，只是时间问题。

（三）处置方案

1) 使用医院日常冷备份数据，对服务器系统进行快速恢复，未备份数据，人工重新录入；

2) 全面检查内网所有设备的密码，修改所有弱口令，包括防火墙、服务器等，禁止使用看似复杂，但常见有规律的弱口令；

3) 尚未部署安全软件的服务器立即部署安全软件，并进行全盘查杀；及时对病毒库进行更新，设置定期进行全面扫描，加强服务器上的病毒清除能力；

4) 采用端口白名单机制，只允许开放特定的业务必要端口，其他端口一律禁止访问，仅管理员 IP 可对管理端口进行访问，如 FTP、数据库服务、远程桌面等管理端口。

六、某三甲医院内网出现大量异常流量被网警通报

（一）场景回顾

2021 年 11 月，某地一家三甲医院被网警通报发现大量异常流量，经自查发现多个挖矿木马和蠕虫病毒，故请求奇安信安服团队排查被攻击服务器并确定攻击源。

（二）事件分析

现场对失陷服务器主机进行溯源分析发现，2021 年 10 月，就已经有多个 IP 对医院内部服务器进行暴力破解的攻击行为。同时，我们在医院服务器上还发现了 Trojan.Agent 木马病毒。对现有失陷服务器进行日志分析，确定攻击者是首先攻破一台服务器，再通过暴力破解进行横向传播，然后在多台服务器和办公终端中，植入挖矿木马和蠕虫病毒等多个恶意服务。

（三）处置方案

1) 对所有失陷主机进行断网处理，重装系统并安装安全软件，其他为失陷主机安装安全软件和专杀工具进行查杀并对可疑恶意服务进行上机排查；

2) 对于出现弱口令的主机强制修改为强口令，对矿池恶意域名进行拉黑封禁处理，并对内部员工进行相关的安全培训；

3) 针对暴力破解的情况，对防火墙必要端口进行阻断控制，同时配置私有 DNS 解析到本地，就不会连接到恶意域名矿池上。

附 录一

2021 全球医疗卫生行业十大网络安全事件

本章以《安全内参》全球新闻素材库为基础，整理了 2021 年全球医疗卫生行业的网络安全大事件。

一、国家医保局发布加强网络安全和数据保护工作的指导意见

2021 年 4 月 6 日，国家医保局发布《国家医疗保障局关于印发加强网络安全和数据保护工作指导意见的通知》（以下简称《通知》），其中明确，到 2022 年基本建成基础强、技术优、制度全、责任明、管理严的医疗保障网络安全和数据安全保护工作体制机制。到“十四五”期末，医疗保障系统网络安全和数据安全保护制度体系更加健全，智慧医保和安全医保建设达到新水平。《通知》明确了医疗卫生行业网络安全工作未来 5-10 年的发展方向：进一步明确和加强网络安全和数据安全保护制度的健全和实施方向，为稳妥推动数据资源开发利用，发挥数据生产要素作用，更好地服务医保政策制定和医保精细化管理提供技术准备。

二、美国医疗服务商遭勒索攻击致系统停顿损失数百万美元

2021 年 1 月，美国佛蒙特州一家医疗服务提供商遭到网络攻击，导致电子健康记录 (EHR) 系统延迟推出，并造成数百万美元的收入损失。总部位于伯灵顿的佛蒙特大学健康网络 (University of Vermont Health Network) 早在 2020 年

10 月就曾受到勒索软件攻击，导致了包括放射科在内的各个部门的延迟。

该网络服务于佛蒙特州的大部分地区和纽约州北部的部分地区。当攻击者袭击了 6 家网络医院时，佛蒙特州州长菲尔·斯科特 (Phil Scott) 认为情况严重到需要部署佛蒙特陆军国民警卫队的联合网络反应小组来帮助恢复工作。

三、巴西医疗保健巨头遭 REvil 勒索软件攻击导致系统中断

2021 年 6 月，巴西最大的医疗诊断公司 Grupo Fleury 遭勒索软件攻击。该公司将其系统下线，业务运营中断，患者无法进行在线诊断或其他临床检查。据消息人士称，Grupo Fleury 此次遭遇的是 REvil 勒索软件攻击，此前该勒索软件攻击过的企业包括巴西的南里奥格兰德法院系统、核武器承包商 Sol Oriens 和全球最大的肉类生产商 JBS。据分析，此次解密赎金至少需要 500 万美金。REvil 软件采用的是双重勒索攻击，即在加密设备之前窃取文件。如果数据被盗，此事件将会造成更严重的影响，因为包含大量患者的个人医疗数据。

四、北爱尔兰发生数据泄露后暂停疫苗在线认证服务

2021 年 7 月，北爱尔兰卫生部发生数据泄露事件后，暂停了其新冠疫苗在线接种认证服务。该政府机构表示，少量用户可能会接触到其他用户的数据，导致他们暂时停止服务。

此前在 2021 年 5 月，爱尔兰卫生服务执行机构（HSE）遭勒索软件攻击，导致 HSE 所有 IT 系统被关闭，其内部电子邮件系统也因此无法使用。爱尔兰政府的国家网络安全中心（NCSC）表示，攻击者使用一年前出现的 Conti 勒索软件实施攻击。HSE 受到攻击的细节未披露，勒索团伙索要大约 2000 万美元的赎金。

五、意大利地方疫苗接种预约系统因网络攻击被迫关闭

2021 年 7 月底，黑客攻击了管理意大利罗马周边的拉齐奥地区 COVID-19 疫苗预约的公司 IT 系统，导致该系统被迫关闭。包括该地区的卫生门户网站和疫苗接种网络的系统在内的所有的系统都被停用，相关部门警告说接种计划可能会受到延误。据安莎社报道，意大利邮政警察和罗马检察官正在调查此事，并可能展开调查以找出攻击的幕后黑手。事件发生前，意大利跟随法国宣布，接种疫苗或提供 COVID-19 免疫证明，将成为参加各种聚集活动的强制要求。

六、美国一 DNA 检测公司敏感数据泄露影响 210 万用户

2021 年 8 月，位于美国俄亥俄州一家进行 DNA 检测服务的 DNA 诊断中心检测到自身系统发生了一起数据泄露事件。黑客利用漏洞，访问了该公司 2004 年至 2012 年期间用户包括姓名、财务帐号、社会安全号码、信用卡 / 借记卡号码及其安全码在内的高度敏感个人数据，其中超过 210 万名用户的敏感个人和财务数据被窃取。该公司表示，没有基因检测数据因此次数据泄露事件而暴露。

七、美国数十家医院诊所系统瘫痪，患者紧急转移

2021 年 8 月，美国医疗连锁机构 Memorial Health System 遭遇勒索软件攻击，致使 IT 系统瘫痪，旗下三家医院无法正常运营。三家医院只能着手将急诊病患转移至卡姆登克拉克医疗中心。除此之外，位于俄亥俄州贝尔普雷市贝尔普雷医学园区一处独立急诊室的重症监护设施也受到了同一波攻势的影响。

八、美国阿拉巴马州婴儿因勒索软件攻击不幸去世

2021 年 9 月，一名因勒索软件攻击去世的婴儿的母亲对医疗中心提起诉讼，认为医疗中心应对此事件负责。半年多前，美国阿拉巴马州 Springhill 医疗中心遭勒索软件攻击，但很快发布通告目前医院运营并没有受到影响，但实际上部分电子设备已失效，这也导致医护人员监测不到婴儿的状况。待发现问题后，婴儿已出现了严重的脑损伤，在持续供氧九个月后去世。医护人员否认是他们造成婴儿死亡，并补充说根据州法律，医院没有法律义务通知病人网络攻击情况。该案预计将于明年 11 月开审，《华尔街日报》表示，如果指控得到证实，这将是勒索软件攻击首次直接导致个人死亡。

九、加拿大卫生网络遭遇史上最严重网络攻击致敏感数据泄露

2021 年 10 月 30 日，加拿大纽芬兰和拉布拉多省（简称纽省）的卫生网络遭到网络攻击瘫痪，导致全省数千人的医疗预约（包括化疗）被取消，多个地方卫生系统被迫重新使用纸张。直到 11 月 4 日，管辖着 13000 名员工的纽省东部地区卫生局才宣布，内部电子邮件系统重新上线运行。

纽省政府于 11 月 9 日在公告中表示，黑客窃取了近 14 年以来众多东部卫生系统数据，包括姓名、地址、医保编号、社会保险在内的多种患者与员工的个人信息，以及拉布拉多 GrenfellHealth 近 9 年以来的敏感内容。有外部专家表示，此次事件具有勒索软件攻击的一切迹象，包括黑客渗透进 IT 网络内部，并要求受害者付款以换取访问恢复。安全专家认为，加拿大应该把这起针对纽省卫生系统的网络攻击视为国家级安全问题。

十、美国一计划生育协会遭勒索攻击，数十万患者个人信息泄露

2021 年 10 月，美国洛杉矶计划生育协会网络系统感染勒索软件，黑客获取了包括数十万名患者个人信息的文件，包括患者姓名、地址、保险信息等基本信息和临床信息、诊断手术和处方信息等敏感医疗信息。计划生育协会不仅提供堕胎服务，还提供生育控制、性病检测、激素治疗等医疗服务，所以患者信息极其敏感和有价值。

附 录二

作者简介

《2022 医疗卫生行业网络安全运营分析报告》是由奇安信行业安全研究中心在多个研究团队的共同帮助下编撰完成的。我们在这里向所有参与报告撰写的研究团队致以诚挚的感谢，同时也对各个团队的研究方向及主要贡献进行简要的介绍。

奇安信行业安全研究中心

奇安信行业安全研究中心（以下简称中心）是奇安信集团旗下专注于行业网络安全研究的机构，为政府、公安、军队、保密、交通、金融、医疗卫生、教育、能源等行业客户及监管机构提供专业安全分析与研究服务。

中心以奇安信集团的安全大数据、全球威胁情报大数据为基础，结合前沿网络安全技术、国内外政策法规，以及每年千余起网络安全应急响应事件的处置经验，全面展开行业级、领域级、国家级网络安全研究。

中心自 2016 年成立以来，已累计发布各类专业研究报告一百余篇，共计三百余万字，在勒索病毒、信息泄露、网站安全、APT、应急响应、人才培养、安全运营等多个领域的研究成果受到海内外网络安全从业者的高度关注。

同时，中心还联合各个专业团队，主编出版了多本网络安全图书专著，包括《走进新安全》、《透视 APT》、《应急响应》、《应急响应技术实战指南》、《工业互联网安全 - 百问百答》、《内生安全 - 新一代网络安全框架》、《红蓝攻防》等，为网络安全知识的深度传播做了重要的贡献。

补天漏洞响应平台

补天漏洞响应平台（https://www.butian.net），成立于 2013 年 3 月，是国内专注于漏洞响应的第三方平台。补天平台通过充分引导民间白帽力量，实现实时的、高效的漏洞报告与响应。

面对复杂多变的网络安全态势和层出不穷的攻击手段，补天平台采用 SRC、众测等方式服务广大企业，以安全众包的形式让白帽子从模拟攻击者的角度发现问题，解决问题，帮助企业树立动态、综合的防护理念，守护企业网络安全。补天平台将多种安全服务有机的整合起来，进一步提升企业的漏洞响应能力、积极防御能力和常态化安全运营能力。

成立 7 年来，补天平台已经成为全中国影响力最大的漏洞响应平台之一，同时也是最活跃的网络安全从业者交流平台之一。通过补天白帽大会、“补天杯”破解大赛、补天城市沙龙、补天校园行，搭建安全从业者开放、分享、成长的平台，把国内外网络安全专家、业界大咖、安全厂商、研究机构聚集到一起，结合多种形式建立网络安全从业者技术生态。同时在实战化的趋势下，人是支撑安全业务的最重要因素，补天平台也成为汇聚海量实战型网络安全人才的资源池。通过提供真实的训练环境，开放实战工具箱和资源，定制专属课程、顶级黑客进行技术教学，依托长期积累，利用独有的技术人才优势，培养出具有顶级技术的网络安全实战型人才，为行业提供强有力的人才保障，提升支撑安全业务的各项能力，应对新形势下的网络安全挑战。

网聚安全力量，为社会提供准确、详实的漏洞情报，实现漏洞的及时发现与快速响应，是补天平台始终坚持并不断履行的社会使命。通过营造实战化的学习环境、建设协同育人的导师制度、构建技能衔接的知识体系培养的实战化人才为企业网络安全贡献力量，为国家安全保驾护航。

奇安信安全托管服务

奇安信安全托管团队，根据安全数据和团队所在地的不同，将安全托管服务业务打造为三种模式：

远程安全托管服务：由奇安信提供集人员、流程、工具结合企业本地自身的安全相关数据来开展的远程托管模式。通过该服务提供 7*24 的安全监测，快速发现和响应客户侧安全产品的各类安全风险事件，协助用户进行事件闭环，同时提供应急值守团队进行应急保障，提升用户运营效率。此服务模式主要适用于中小企业场景。

现场托管服务：由奇安信配合企业安全部门共同进行安全运营架构、包括运营组织搭建，事件响应流程，运营平台及工具进行设计，通过外购或自研安全运营、流程管理等平台及设备、规划对应的工作场地，招募能胜任的专业人员开展“企业自治”的安全托管模式。此模式需要企业内部的管理支撑及大量的投资方可开展，大多适用于大型企业场景。

城市安全托管服务：奇安信与政府合作，或与当地大型的本地化合作伙伴来合作，为智慧城市提供统一的、规范化、流程化的管理与运维服务，减少了人工运维投入，降低了信息化管理维护成本。实现系统资源的统一规划、统一建设、按需调配、即需即用、有效共享。此服务模式有效实现智慧城市背景下网络空间安全的高效治理、集中统筹和集约化运营，为城市网络安全提供了有力保障。

奇安信网络安全应急响应服务

奇安信安全服务以攻防技术为核心，聚焦威胁检测和响应，通过提供咨询规划、威胁检测、攻防演习、持续响应、预警通告、安全运营等一系列实战化的服务，在云端安全大数据的支撑下，为客户提供全周期的安全保障服务。

应急响应服务致力于成为“网络安全 120”。自 2016 年以来，奇安信已积累了丰富的应急响应实践经验，应急响应业务覆盖了全国 31 个省（自治区、直辖市），2 个特别行政区，处置政企机构网络安全应急响应事件超过三千起，累计投入工时 37000 多个小时，为全国超过两千家政企机构解决网络安全问题。

奇安信还推出了应急响应训练营服务，将一线积累的丰富应急响应实践经验面向广大政企机构进行网络安全培训和赋能，帮助政企机构的安全管理者、安全运营人员、工程师等不同层级的人群提高网络安全应急响应的能力和技术水平。奇安信正在用专业的技术能力保障着企业用户的网络安全，最大程度地减少了网络安全事件所带来的经济损失，并降低了网络安全事件造成的社会负面影响。

应急响应 7×24 小时热线电话：95015。

安全内参

《安全内参》是专注于网络安全产业发展和行业应用的高端智库平台，依托于专业的安全团队和数千位国内外产业和行业智库的专家团队，为网络安全相关政府主管、行业、企业和机构的管理者、决策者和从业者提供全球视野、高价值的安全知识和安全智慧，致力于成为网络安全首席知识官。

安全内参地址：https://www.secrss.com/info/about

官网二维码

报告二维码

应急响应

7×24小时热线电话：95015