

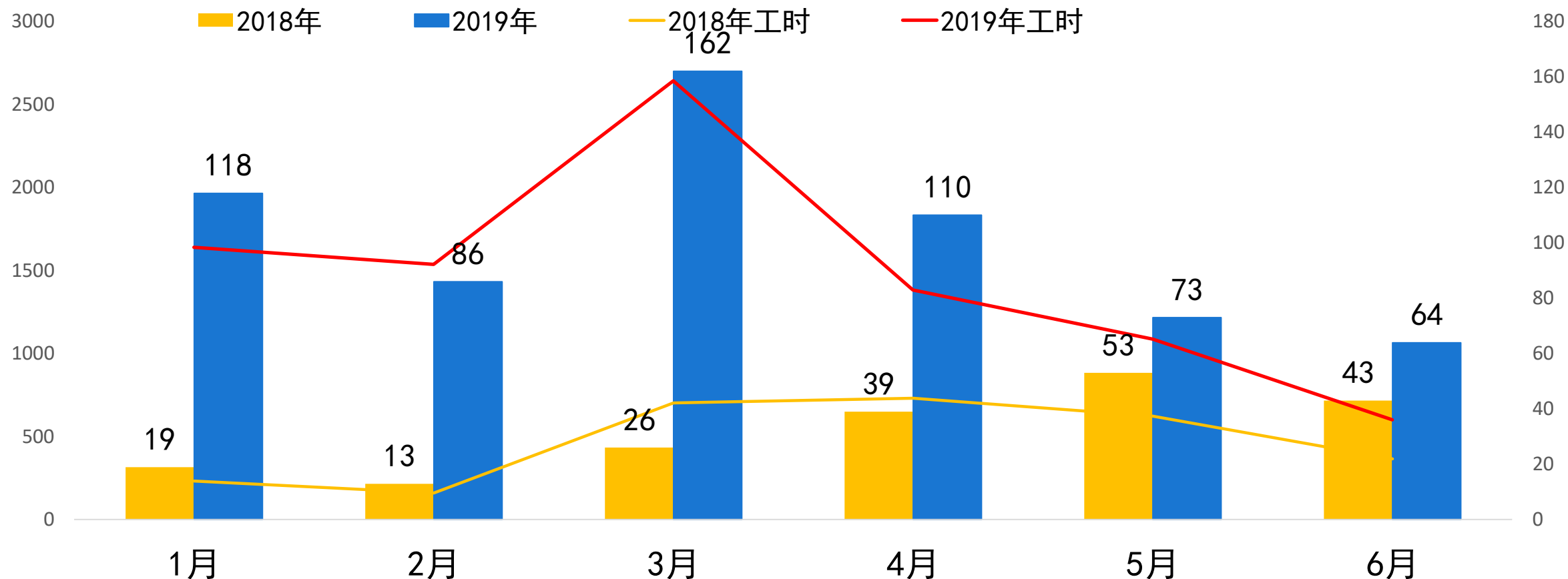


# 从应急响应看医疗卫生 行业网络安全现状

## 目录

- 应急响应总体形势
- 医疗卫生行业应急总体形势
- 医疗卫生行业典型案例
- 医疗卫生行业安全建议

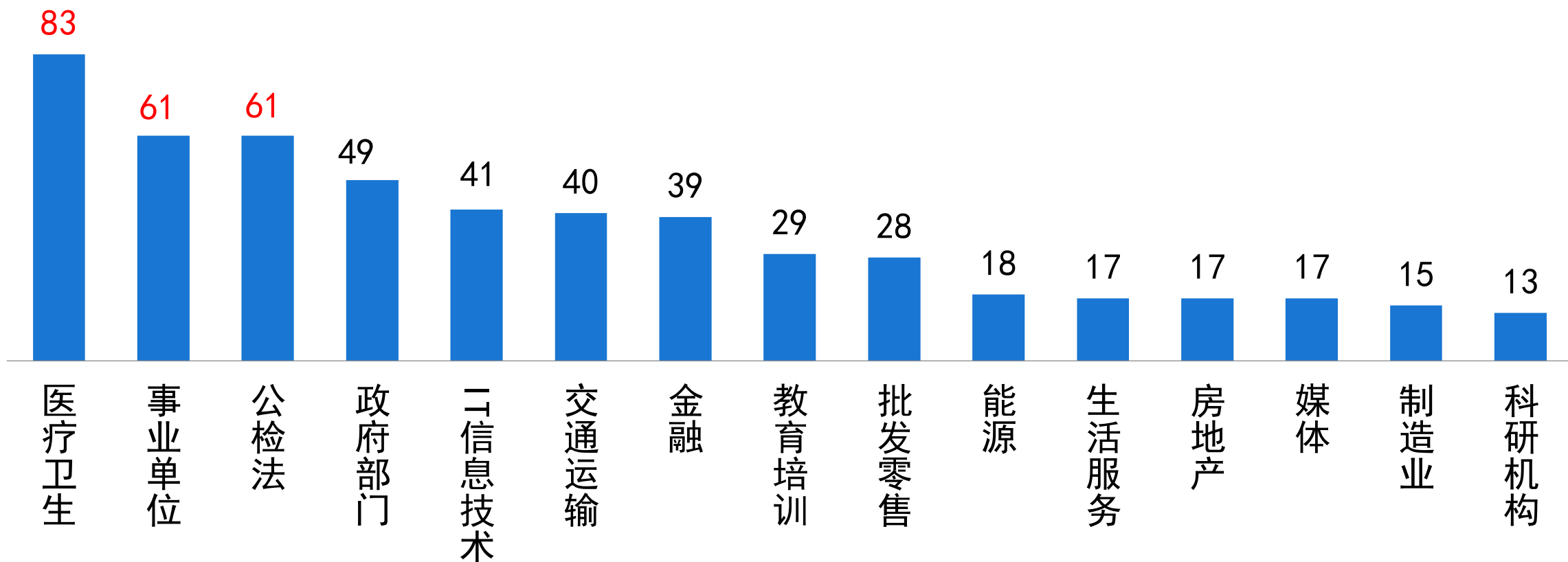
## 2019上半年应急响应月度分布



2019年上半年奇安信集团安服团队应急响应服务需求**613**起，同比2018年上半年增长近**69%**。

**我国网络安全形势依然严峻。**

## 2019上半年应急响应行业现状分布 (TOP15)



2019年上半年应急处置事件最多的行业TOP3分别为:

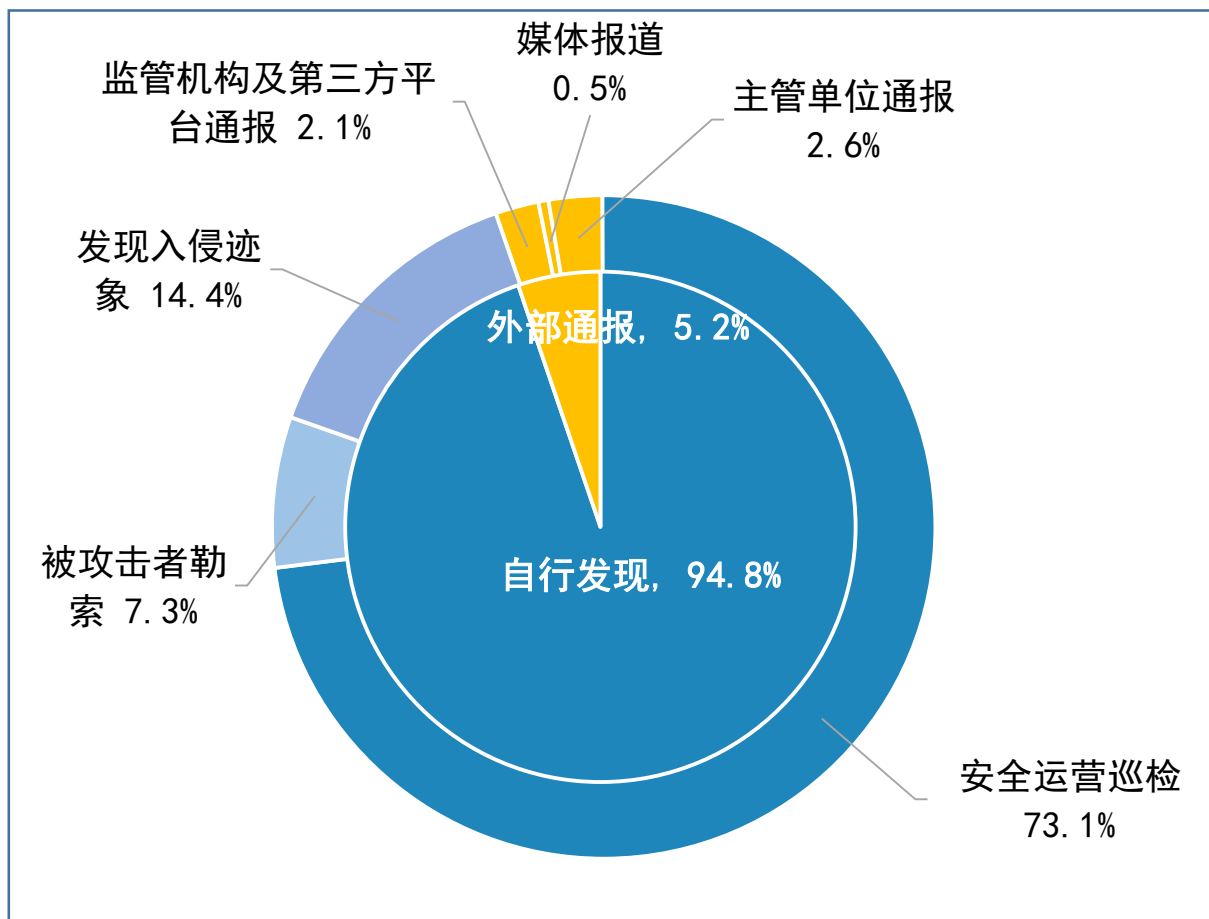
**医疗卫生行业 (83起)** , 事件处置数占应急处理事所有行业的**13.5%**;

**公检法行业 (61起)** , 事件处置数占应急处理事所有行业的**7.5%**;

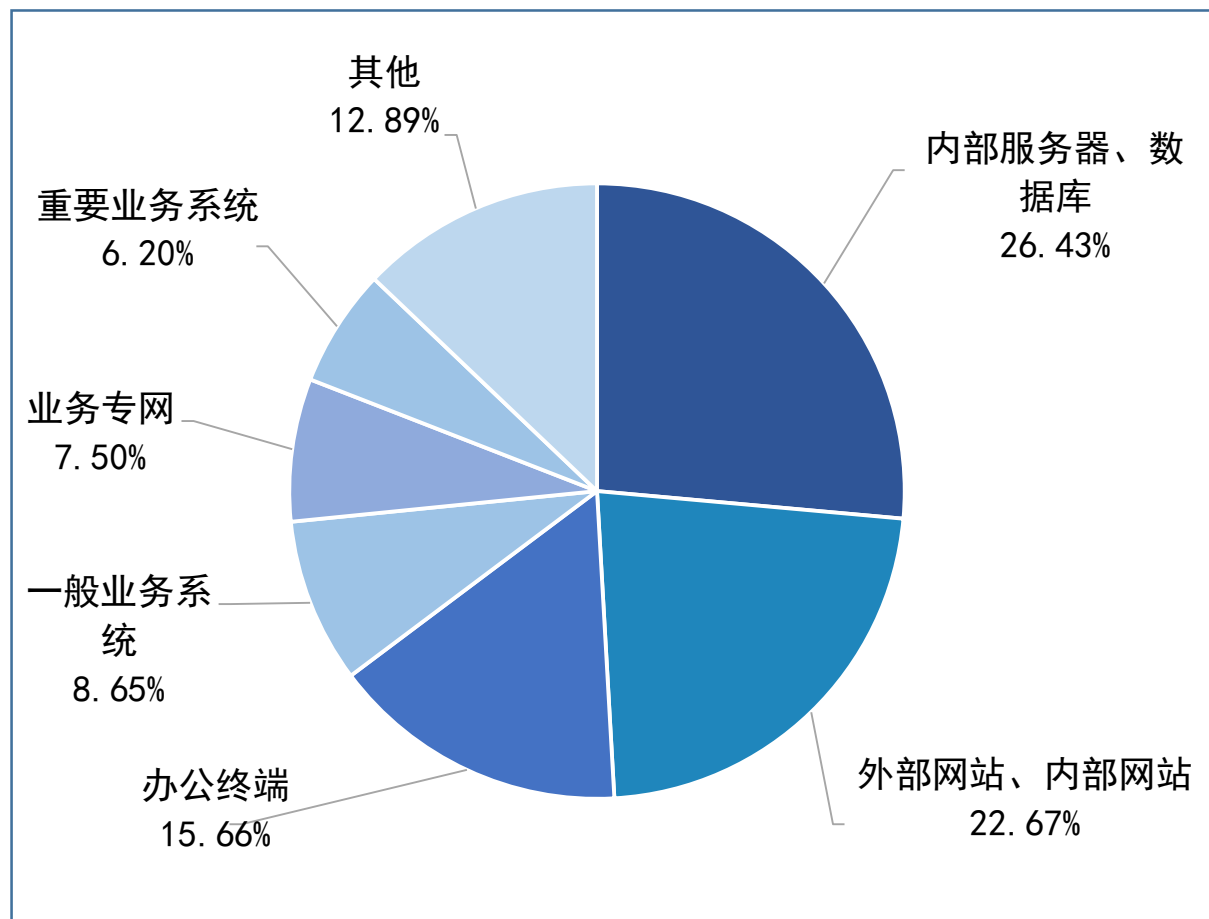
**事业单位 (61起)** , 事件处置数分别占应急处理事所有行业的**7.5%**。

## 2019上半年应急事件受害者分析

### 政府机构、大中型企业应急攻击事件发现分析

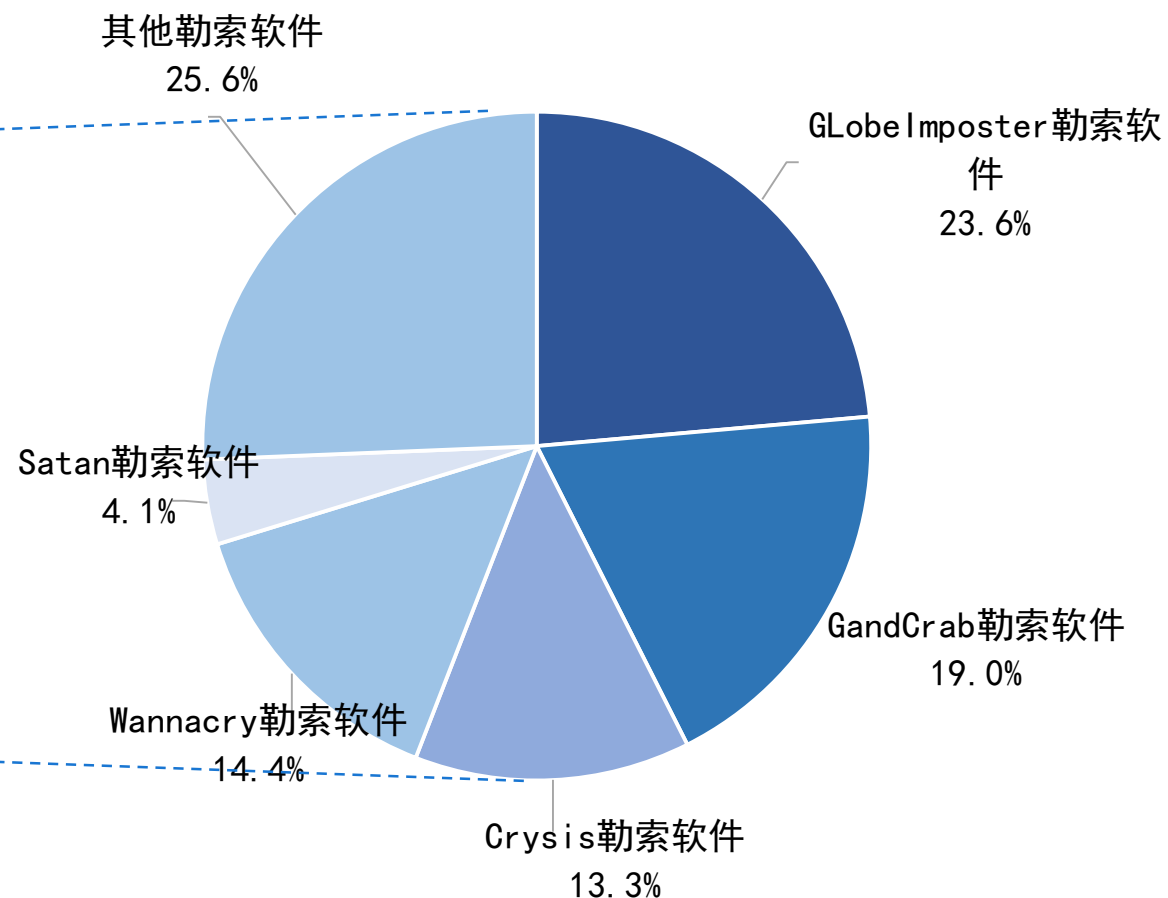
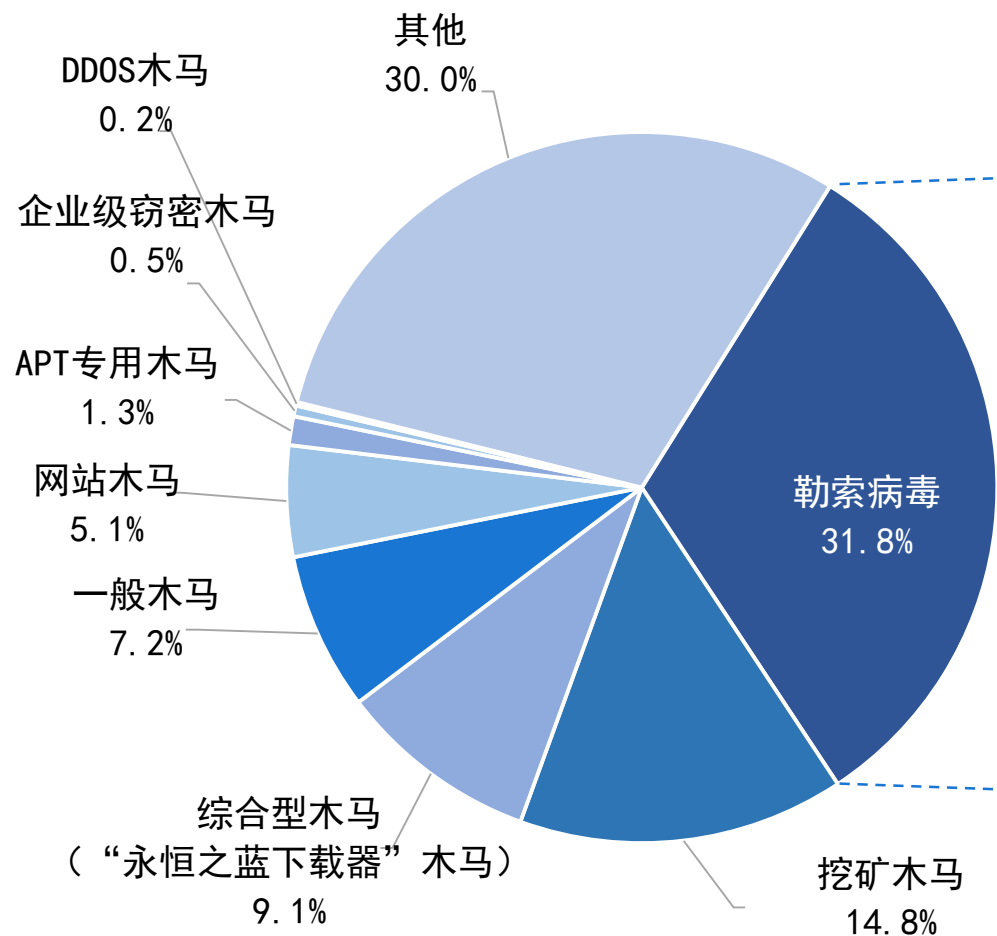


### 政府机构、大中型企业应急影响范围分布影响



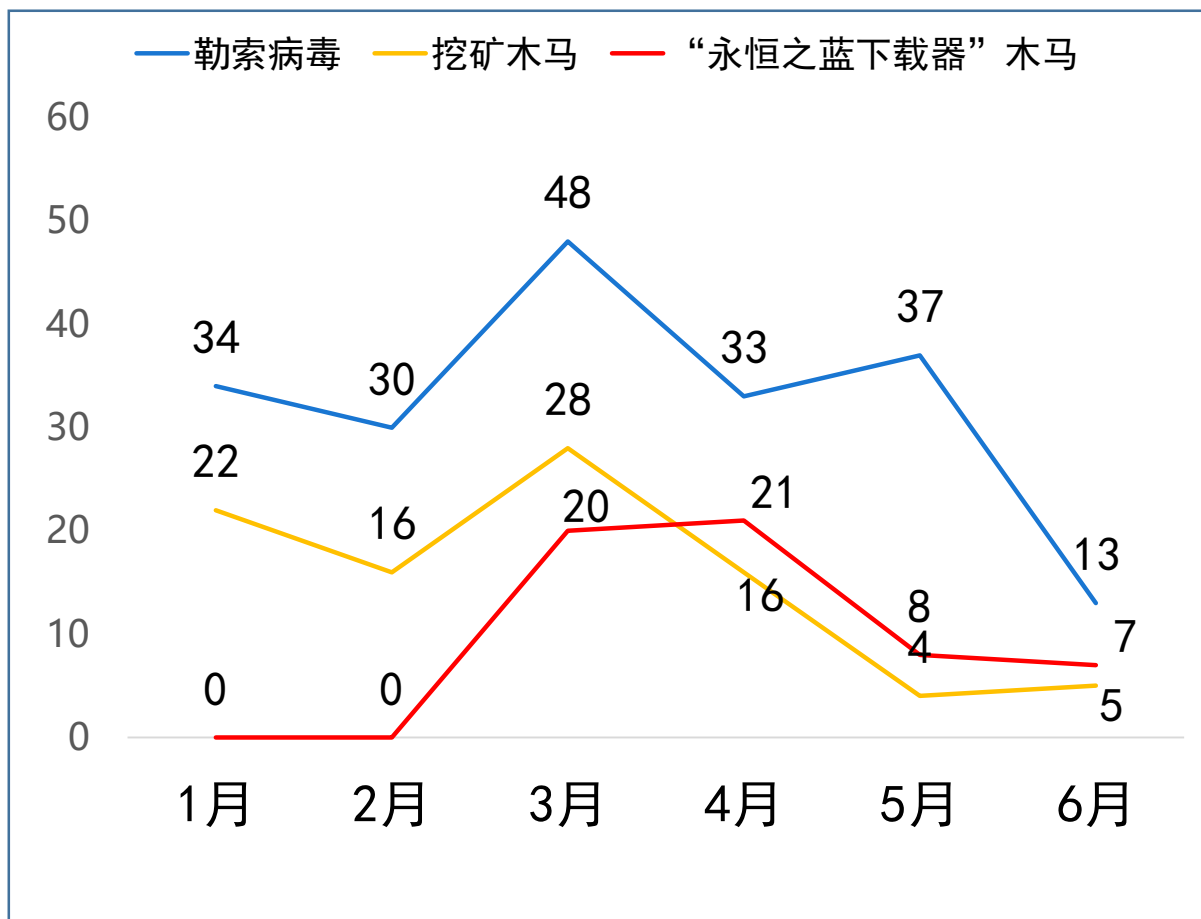
## 2019上半年应急事件攻击者分析

政府机构、大中型企业应急遭受攻击常见木马类型分析

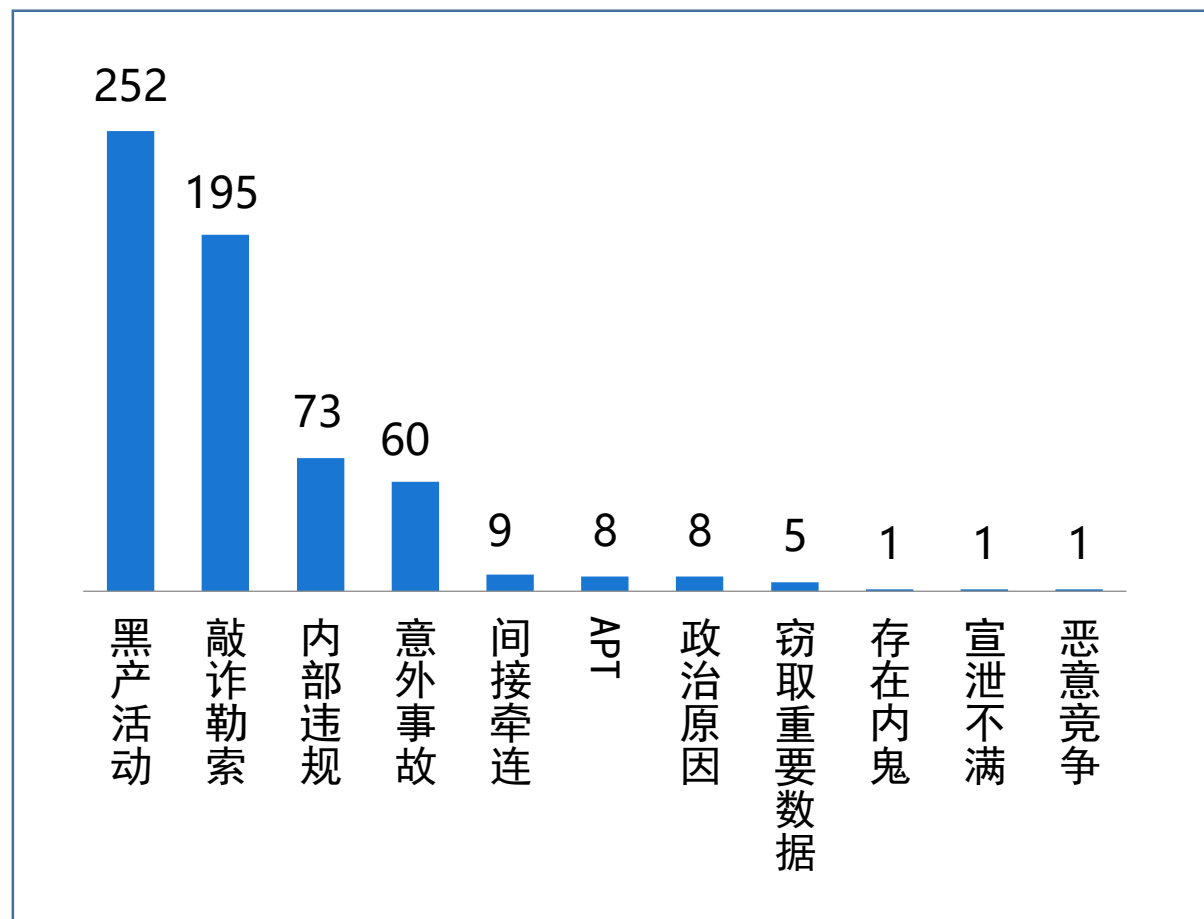


## 2019上半年应急事件攻击者分析

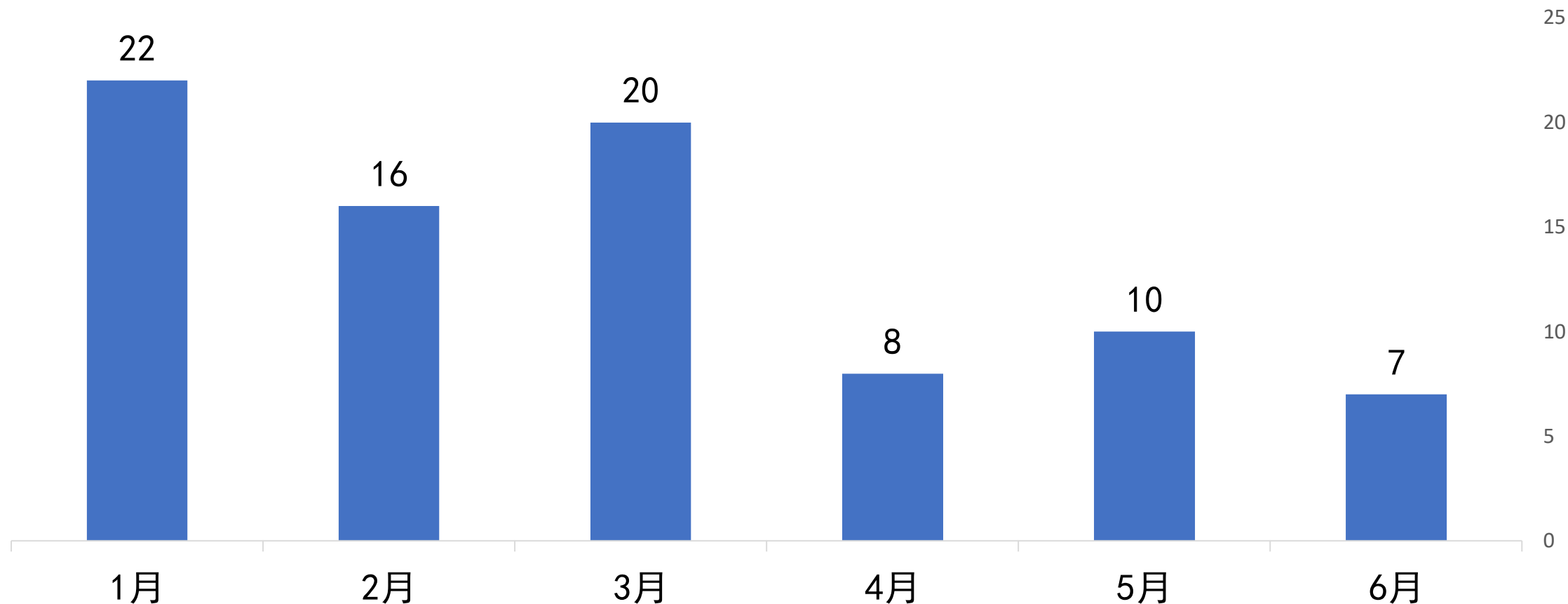
### 应急响应木马类型TOP3月度趋势分析



### 政府机构、大中型企业应急攻击意图分布情况



## 医疗卫生行业应急响应月度分布

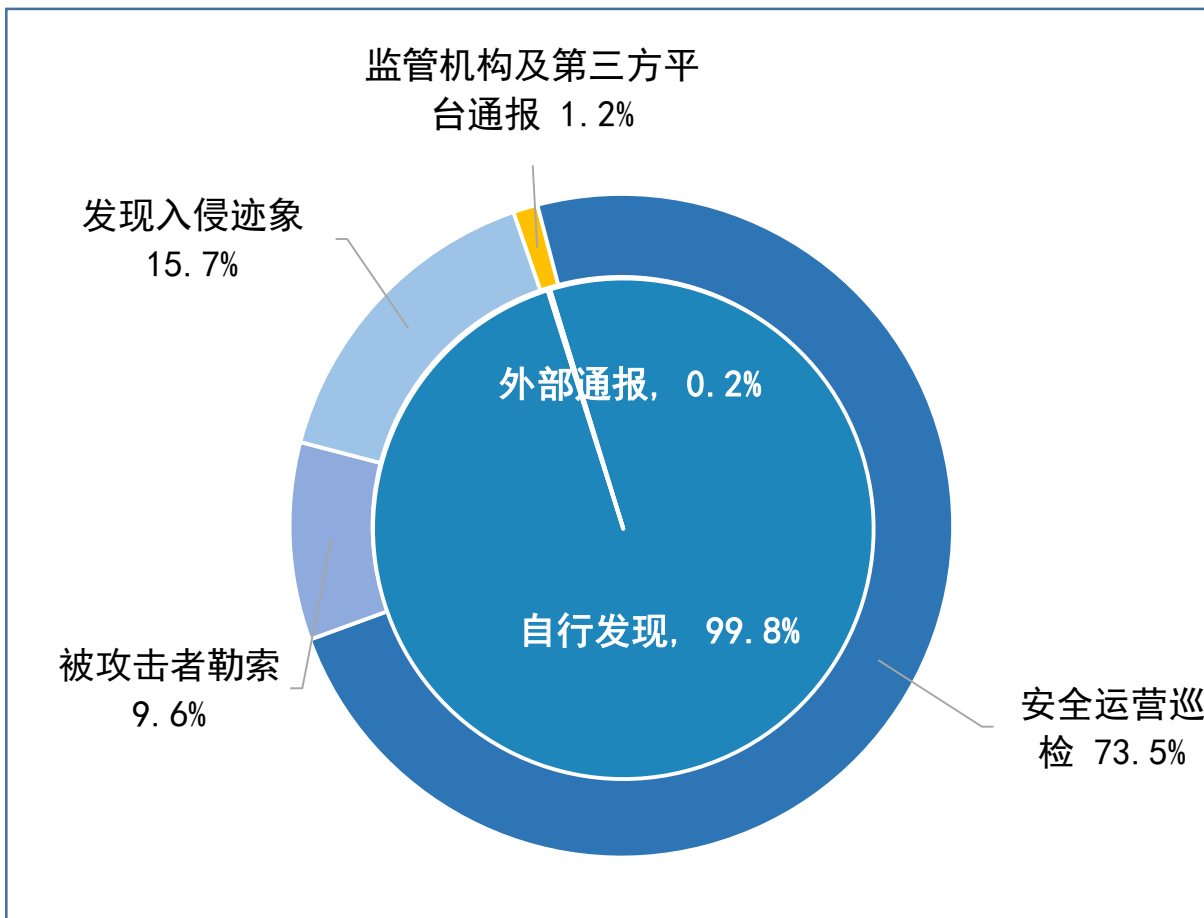


2019年上半年奇安信集团安服团队应急响应医疗卫生行业救援服务**83**起，占2019年上半年各行业应急事件的**13.5%**。

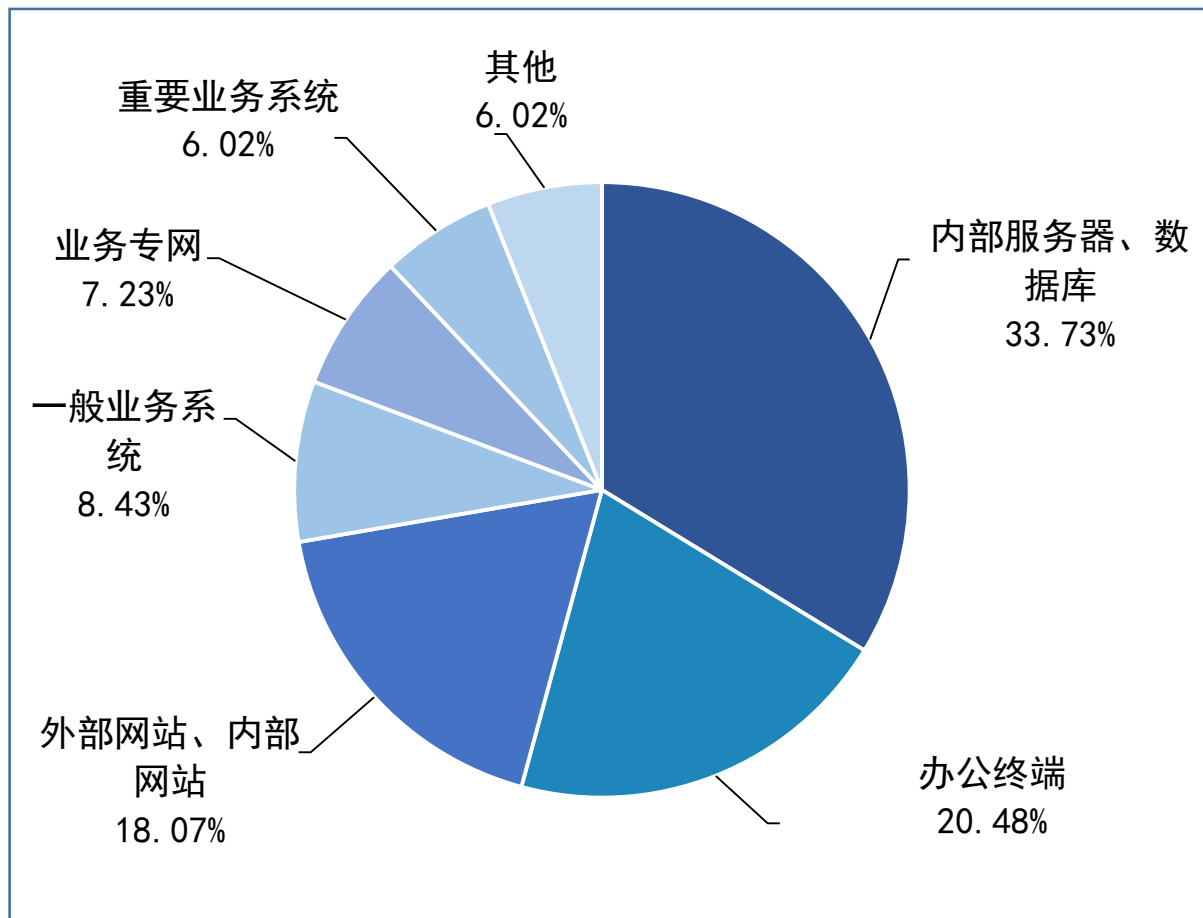
**1月**、**3月**应急次数最多，分别占上半年医疗卫生行业应急总数的**26.5%**、**24.1%**。



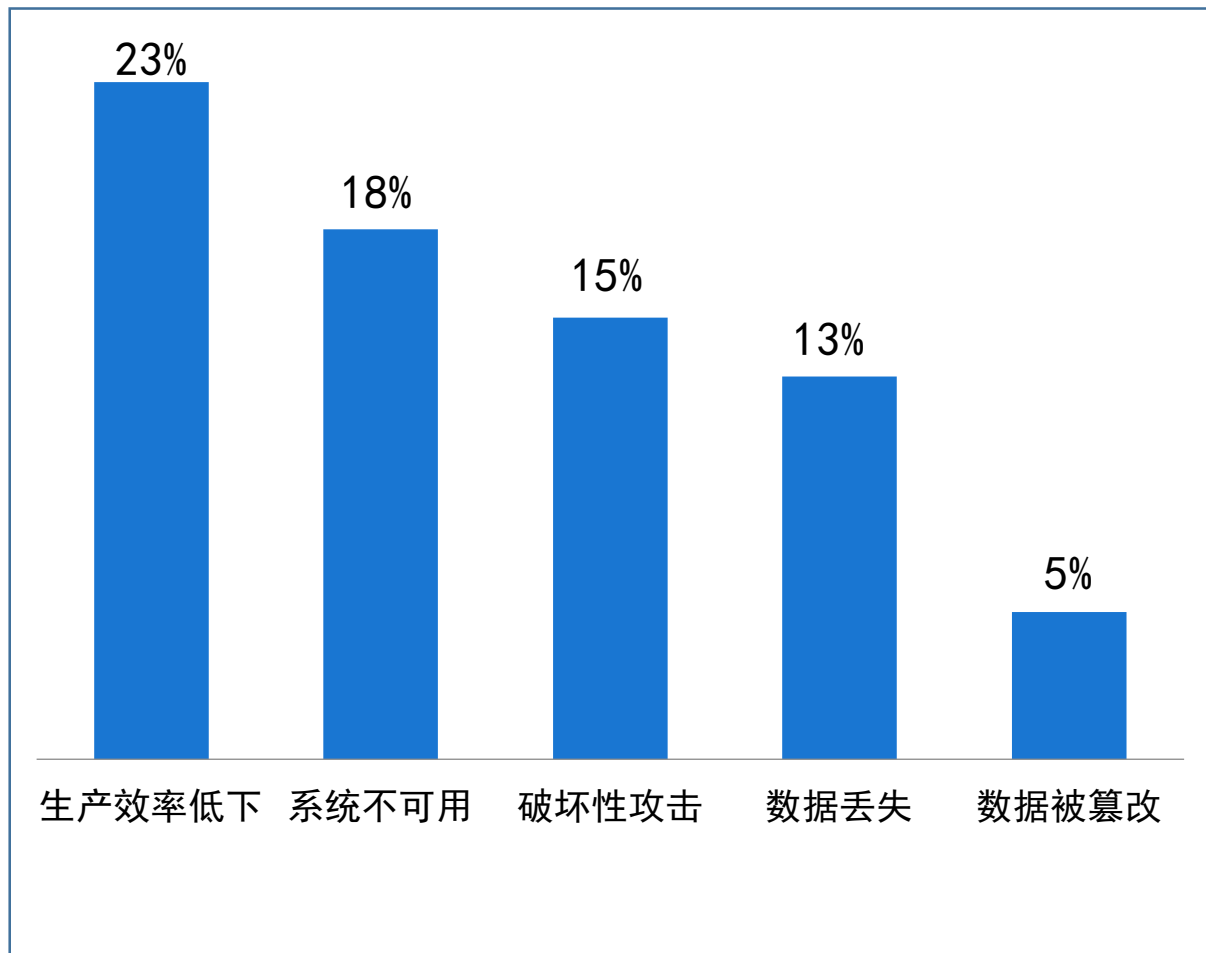
## 医疗卫生行业应急攻击事件发现分析



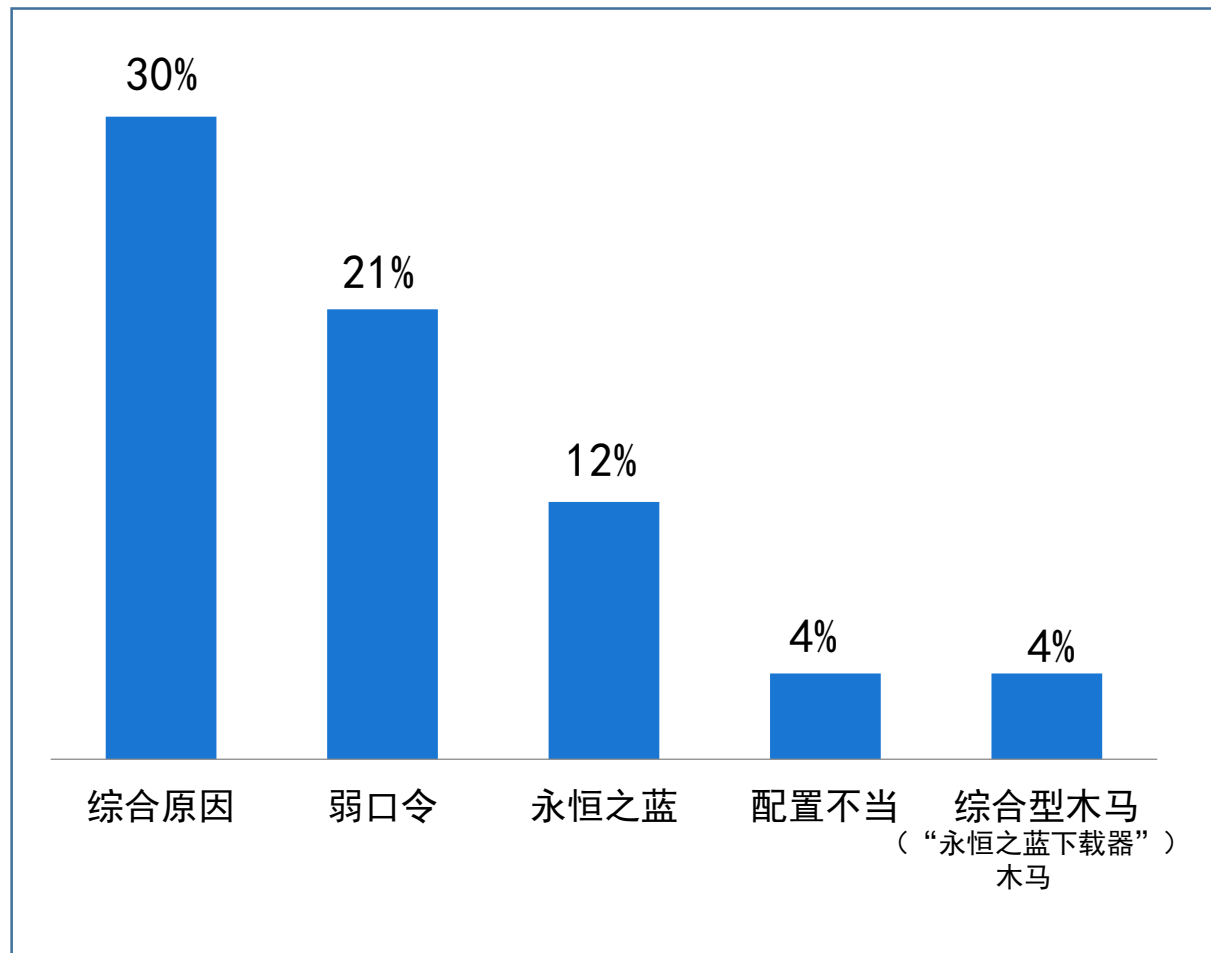
## 医疗卫生行业应急影响范围分布影响



## 医疗卫生行业应急攻击现象统计分析 (TOP5)

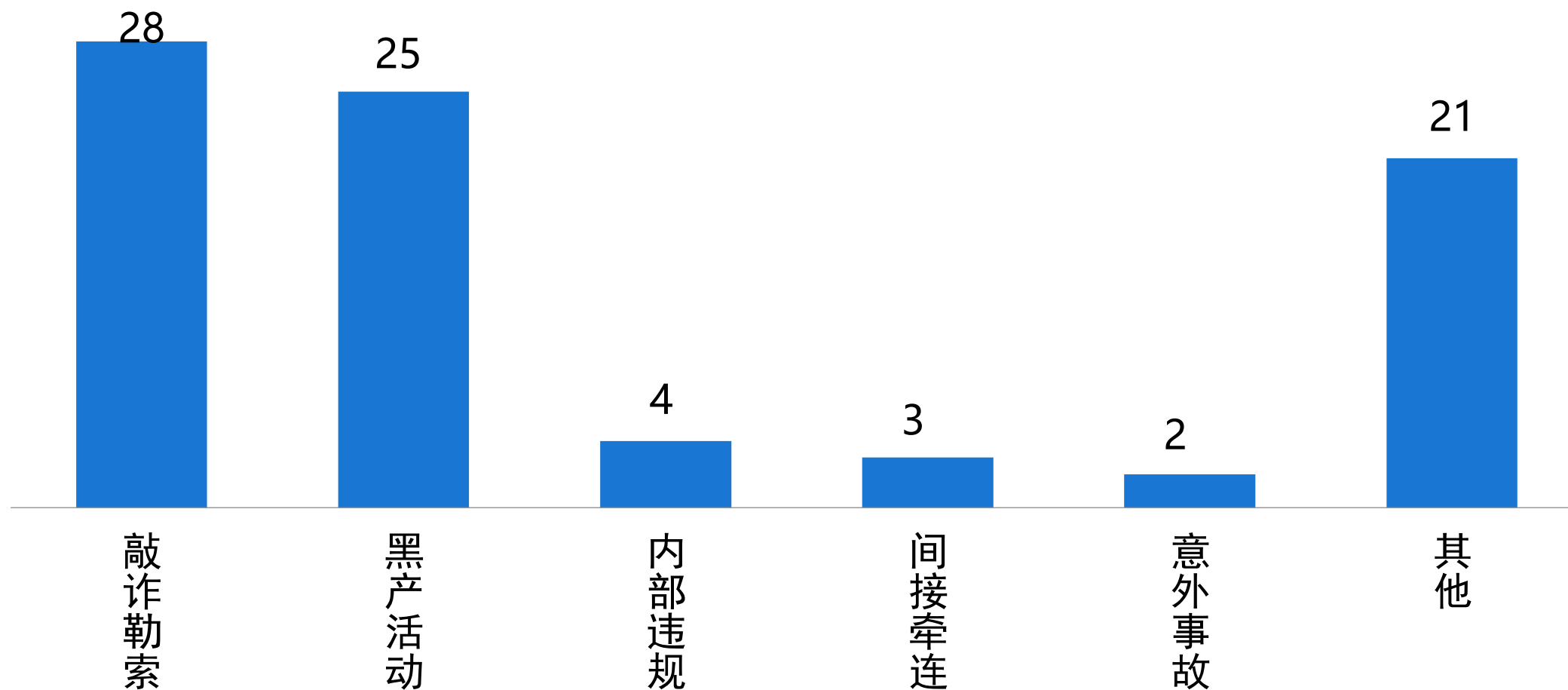


## 医疗卫生行业应急被攻陷原因统计分析 (TOP5)

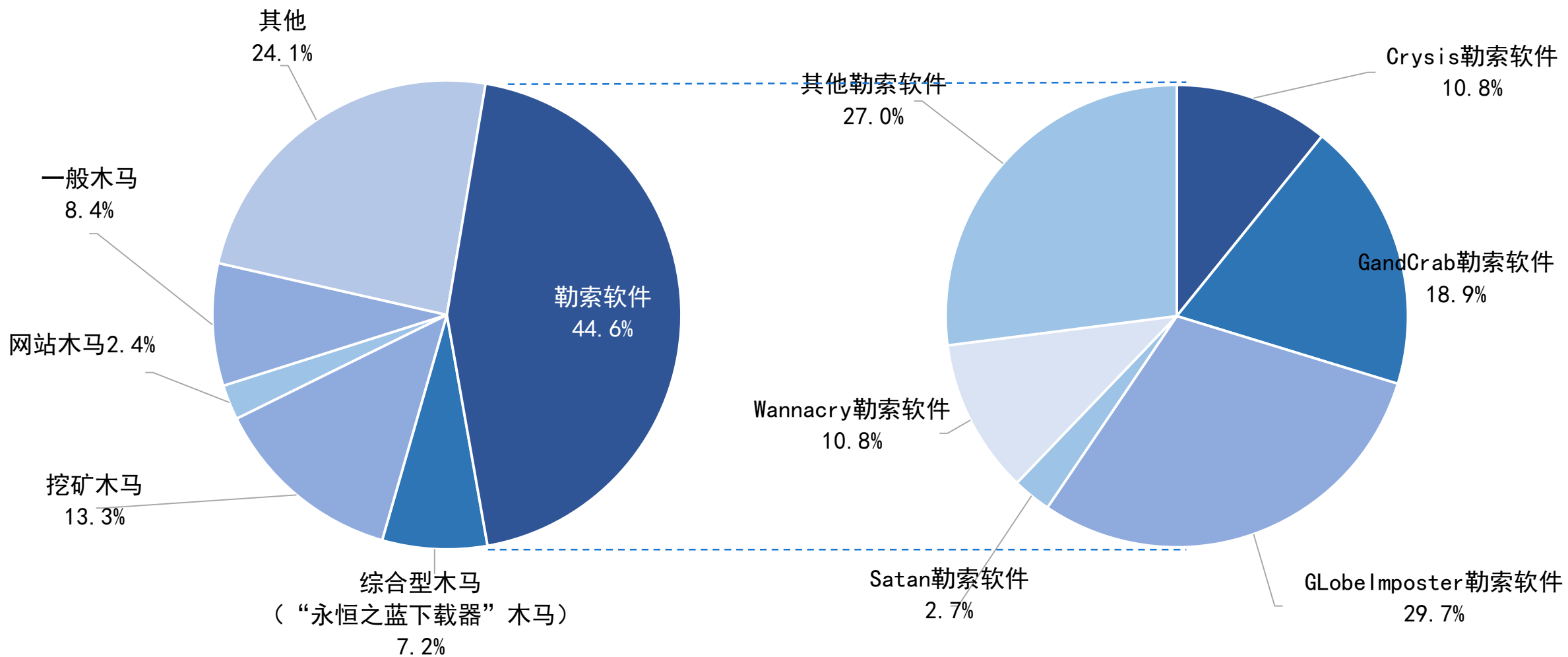


# 医疗卫生行业应急总体形势

## 2019上半年医疗卫生行业应急攻击意图分布情况



## 医疗卫生行业应急遭受攻击常见木马类型分析



## 典型案例一：某省人民医院内网勒索病毒GANDCRAB处置

2019年2月，安服应急团队接到某省人民医院内网爆发GANDCRAB v5.0.4勒索病毒的应急请求，多台服务器与工作用机的文档被加密，业务无法正常运行。

应急人员通过对现场情况进行分析，确定此次感染勒索病毒事件是攻击者从外网进入，利用跳板机分发勒索病毒，从而感染内网机器的人为攻击事件。攻击者在凌晨工作人员休息的时间段内发起攻击，获取FTP服务器权限并通过RDP远程桌面爆破获取内网其他机器权限。另一方面，攻击者使用FTP服务器通过IPC协议暴力破解成功登录了趋势服务器。攻击手法非常专业，为了FTP服务器被攻陷不被发现，攻击者在获取机器权限后清除了系统日志和攻击工具，其使用的勒索病毒也具有自删除功能，使分析人员无法进一步追溯。

## 典型案例二：某单位专网勒索病毒GlobeImposter处置

2019年3月，国内多家医院感染GlobeImposter勒索病毒事件，安服应急响应团队接到某省多家医院服务器遭受攻击事件的应急请求，经分析此次攻击是发生在该省同一卫生专网的GlobeImposter勒索病毒事件，针对此专网的攻击影响到该省五十多家市县医院。

应急响应人员通过对被感染设备进行分析处置，发现此次医院事件是因为该省在同一卫生专网内横向传染，其攻击手段与2018年的事件类型一致，属常规攻击事件，不具有行业属性。该攻击方式为定向爆破和投递勒索，通过RDP远程桌面攻击服务器，利用ProcessHacker结束杀毒软件进程，并利用其它黑客工具如扫描器、密码抓取工具进行进一步攻击，随后执行勒索软件，文件被加密，病毒感染后的主要特征包括windows服务器文件被加密、加密后缀 \*.snake4444。

## 典型案例二：某单位专网勒索病毒GlobeImposter处置




## 典型案例三：某附属医院“永恒之蓝下载器”木马处置

2019年4月，安服应急响应团队接到客户应急请求，某附属医院网内大约1000多台终端和服务器存在大量病毒，客户机不定时重启、蓝屏，严重影响业务系统的正常运行。

应急人员通过对相关进程、文件、服务进行排查分析后，判断客户内网失陷是由于感染“永恒之蓝下载器”木马，导致病毒泛滥。通过检查客户现场内网失陷主机，发现现场主机系统均未安装杀毒防护软件，C:\Windows目录下存在大量以随机字符命名的.exe文件，并在系统服务中发现大量该exe对应的服务。在分析天眼设备抓取流量时，发现内网共存在11种病毒，包括蠕虫病毒、挖矿病毒、勒索病毒、远控木马、僵尸网络等多种病毒，且发现主机高危端口如135、137、138、445端口均为开启状态并存在传播病毒的行为。除此之外，应急人员在检查过程中发现客户sqlserver数据库管理员账户密码与网内所有服务器均使用同一种密码，且该数据库服务器未安装任何安全防护设备，使得木马快速在内网扩散，并存在大量外连行为，导致大量机器沦陷。



1. 系统、应用相关用户杜绝使用弱口令，应使用高复杂强度的密码，尽量包含**大小写字母、数字、特殊符号**等的混合密码，加强管理员安全意识，禁止密码重用的情况出现；
2. 禁止服务器主动发起外部连接请求，对于需要向外部服务器推送共享数据的，应使用**白名单**的方式，在出口防火墙加入相关策略，**对主动连接IP范围进行限制**；
3. 有效加强访问控制ACL策略，细化策略粒度，按区域按业务严格限制各个网络区域以及服务器之间的访问，**采用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；
4. 部署高级威胁监测设备，及时发现恶意网络流量，同时可进一步加强追踪溯源能力，对安全事件发生时可提供可靠的追溯依据；
5. 配置并开启相关关键系统、应用日志，**对系统日志进行定期异地归档、备份**，避免在攻击行为发生时，导致无法对攻击途径、行为进行溯源等，加强安全溯源能力；
6. 建议在服务器或虚拟化环境上部署虚拟化安全管理系统，提升防恶意软件、防暴力破解等安全防护能力；
7. 建议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；
8. **定期开展**对系统、应用以及网络层面的安全评估、渗透测试以及代码审计工作，主动发现目前系统、应用存在的安全隐患；
9. 加强日常安全巡检制度，定期对**系统配置、网络设备配合、安全日志以及安全策略落实情况**进行检查，常态化信息安全工作；

The background features a dark blue color with a subtle grid pattern. Overlaid on this are several large, flowing, wave-like shapes in a lighter shade of blue, creating a sense of movement and depth.

# THANKS

**2019 北京网络安全大会**  
2019 BEIJING CYBER SECURITY CONFERENCE