安徽文达信息工程学院
网络信息中心
网络安全月报（三月）

报告类型： 网络安全

报告周期： 2026-03-01 09:08:00 - 2026-03-31 08:18:00

报表项内容：

- 网络及安全风险概况
- 网络流量详情
- 应用统计及风险详情
- Web 活动及风险详情
- 网络风险威胁详情
- 威胁说明
- 网络安全防范提示与工作建议

1. 网络及安全风险概况

- 总流量环比增长 **2000.77%**，主要系开学后师生使用人数显著增加，需进一步优化资源配置以保障网络稳定运行。
- 活跃应用环比无明显变化，业务结构整体保持稳定。。(同比正负 10%以内)
- 上一周期 URL 访问未发现高风险行为，访问态势整体可控。
- 网络威胁事件环比增长 **170.94%**，初步判断或因威胁攻击扩散、处置响应时效性不足等因素导致，需尽快开展专项安全处置，防范业务中断、数据泄露等安全事件发生。
- 3 月共计在校内通报网络安全事件 **3 起**，涉及后勤集团、团委、教务处等部门，相关单位需进一步强化内部网络安全防范与管理。

网络概览

531.57 TB
设备总流量

网络应用

1326
个活跃应用

49
Web 资产

103
高风险应用

9
个中高风险

网络威胁

182423
网络攻击

22391
恶意软件

289
扫描

5
拒绝服务

2821
网络钓鱼

0
垃圾邮件

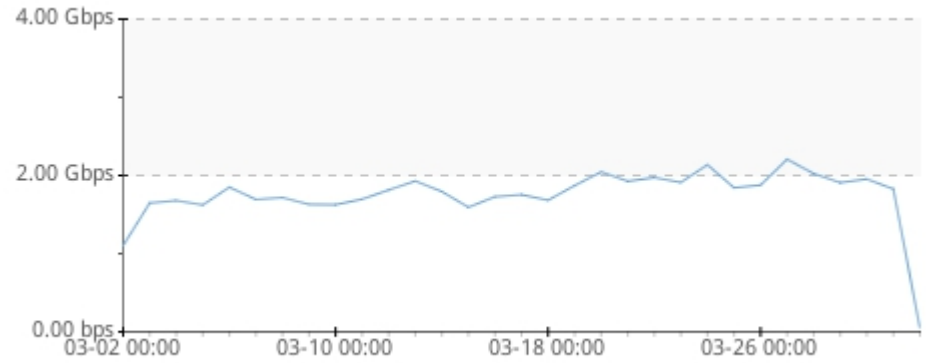
2. 网络流量详情

网络流量反映网络使用的整体情况，通过相关流量统计，能够有效了解链路带宽的利用情况，主要的访问去向，以及流量管理的健康程度。

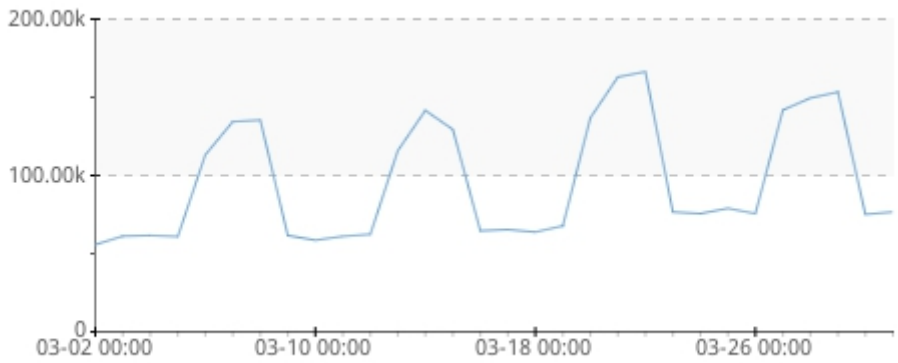
主要发现

- 统计期间整机平均流量 1.81 Gbps，峰值流量 2.21 Gbps，发生在 2026-03-27 00:00。
- 统计期间整机平均并发会话 96242，峰值并发会话 166387，发生在 2026-03-22 00:00。

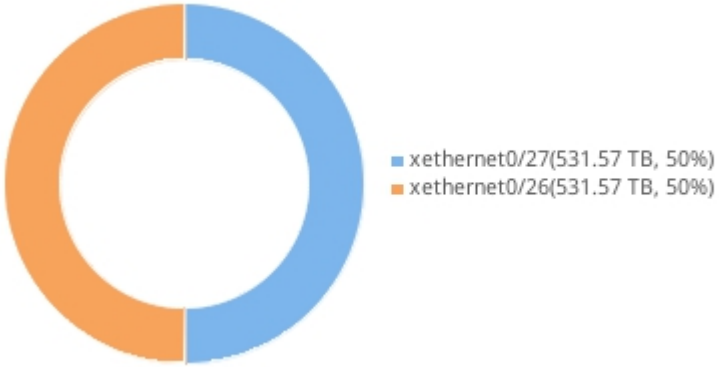
总流量趋势



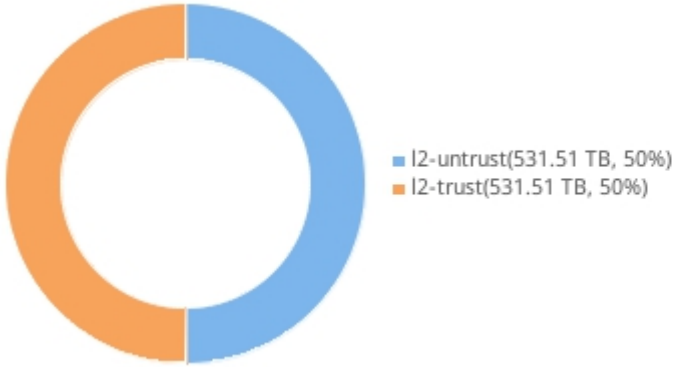
并发会话趋势



接口流量统计分布



安全域流量统计分布



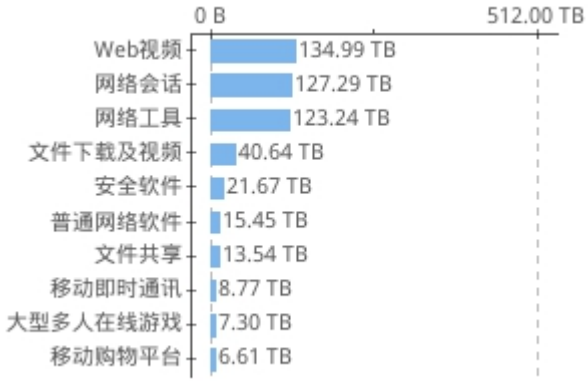
3. 应用统计及风险详情

应用程序可能会引入风险，例如病毒木马传播、传输敏感数据、消耗带宽。需要全面掌握内网的主要业务应用使用情况，根据实际的网络环境状态进行有效调整。

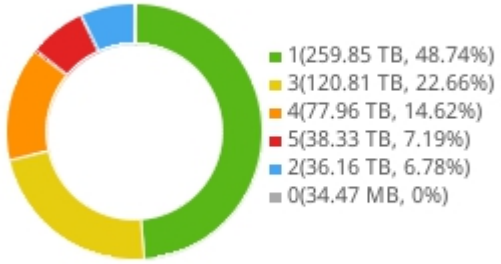
主要发现

- 总共使用 1326 款应用程序，会造成潜在的业务和安全挑战。这是因为关键功能转向外部而不受企业控制，员工使用与工作无关的应用程序，或者网络攻击者使用这些应用程序来传输威胁和窃取数据。
- 在网络上发现了诸如 HTTPS, HTTP, 哔哩哔哩等高风险应用程序，由于存在滥用的可能性，应予以调查。

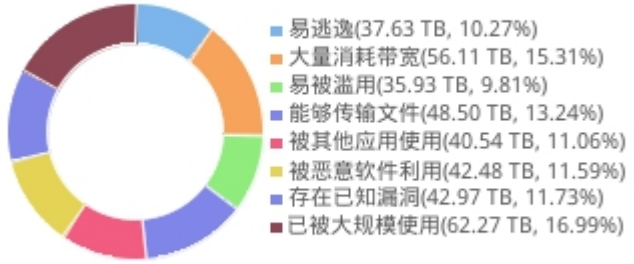
应用子类别排名



应用风险等级分布



应用特征分布



应用列表 TOP10

风险等级	应用名称	应用子类别	应用技术	总流量
1	抖音短视频	Web 视频	客户端服务器	87.57 TB
4	HTTPS	网络会话	基于浏览器	54.18 TB
1	腾讯网	网络工具	客户端服务器	49.77 TB
5	HTTP	网络会话	网络协议	34.98 TB
1	UDP 下载及视频	文件下载及视频	网络协议	27.08 TB
3	Windows 自动更新	安全软件	客户端服务器	20.94 TB
3	腾讯视频	Web 视频	基于浏览器	15.91 TB
3	字节跳动	普通网络软件	客户端服务器	14.08 TB
1	TCP 下载及视频	文件下载及视频	网络协议	13.56 TB
1	WebRTC	网络会话	基于浏览器	11.88 TB

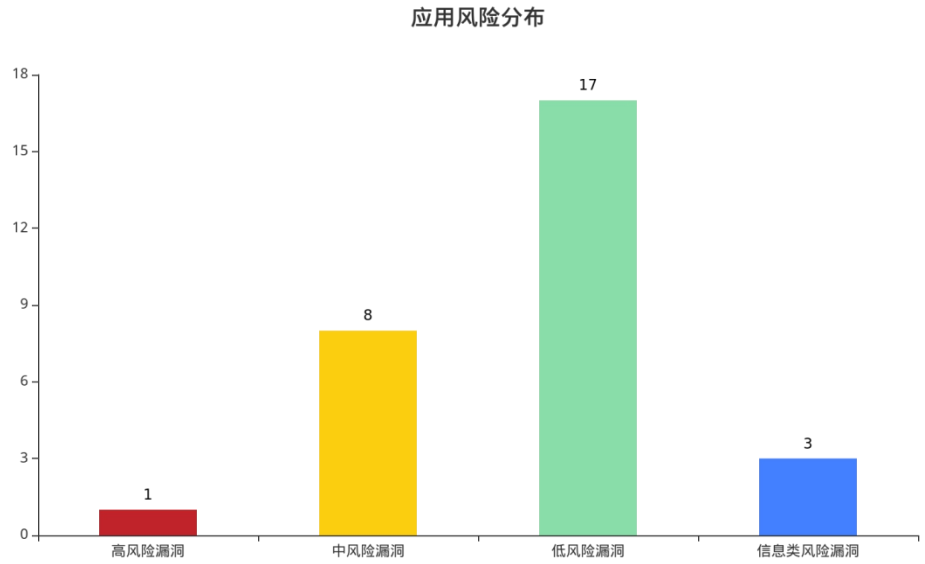
4. web 活动及风险详情

Web 是网络威胁入侵的途径之一，高风险的网站访问极易带来安全隐患，热门网站类型的访问能够体现网络行为的基本情况和整体状态，了解网络带宽的主要应用，避免无谓的带宽消耗。

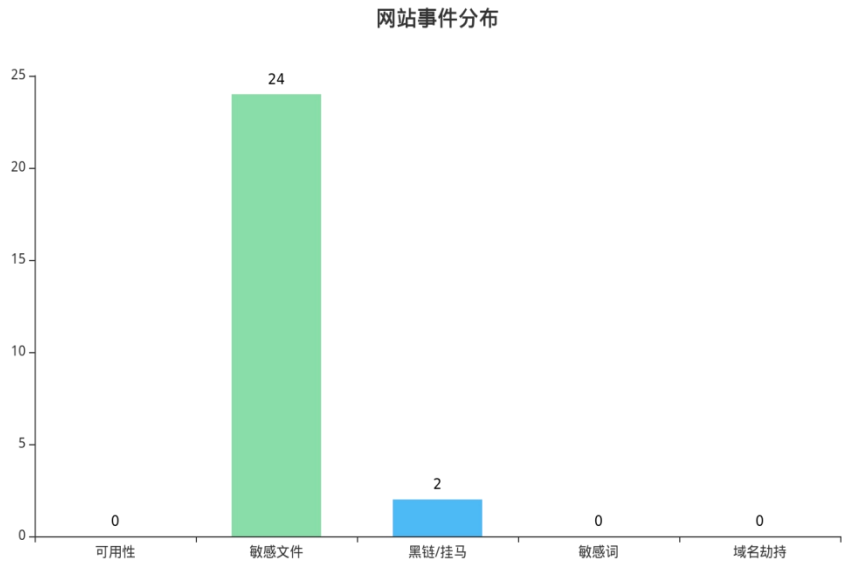
主要发现

共发现 49 个 web 资产，识别出了其中网站的中间件，程序语言以及 web 框架等信息。共发现 1 个高危风险漏洞，8 个中危风险漏洞。共发现 0 个敏感词，24 个敏感文件，2 个黑链，0 个网站篡改，0 个域名劫持、2 个网站可用性故障（目前已恢复）。

应用风险分布



网站事件分布



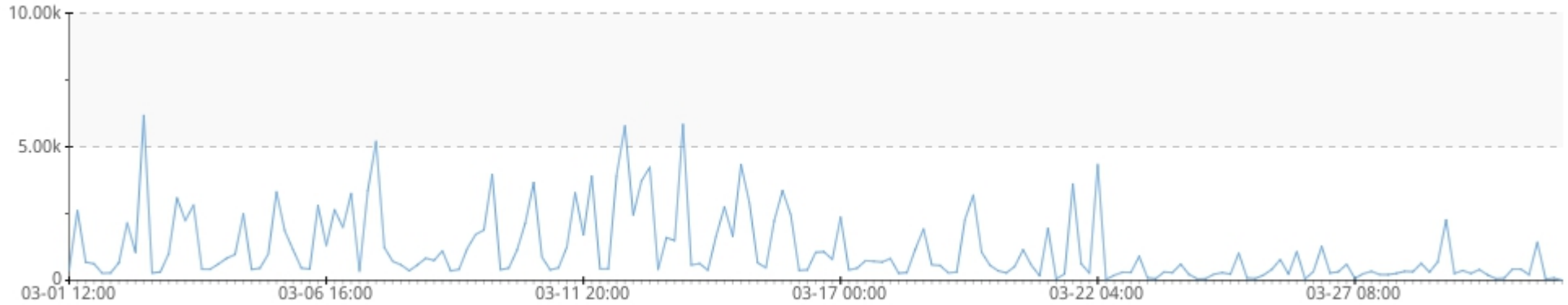
5. 网络风险威胁详情

网络入侵攻击、APT 攻击、网络钓鱼、垃圾邮件、网络传播病毒木马统称为网络威胁，通过了解当前网络中存在的网络威胁，以掌握网络风险程度，并根据具体情况采取相应的安全处置措施。

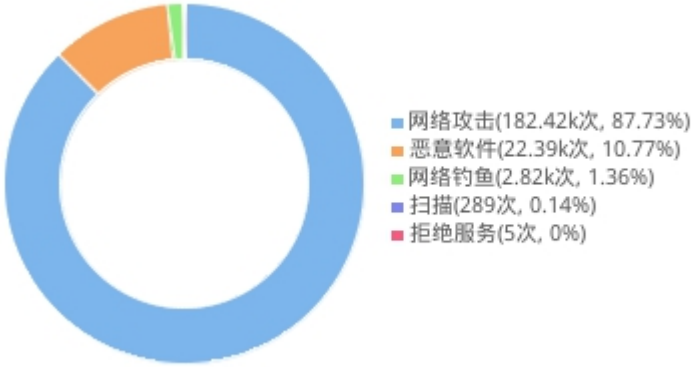
主要发现

- 周期内共产生 207929 次威胁行为，其中网络攻击占比 87.73%，恶意软件占比 10.77%，网络钓鱼占比 1.36%。
- 2026-03-02 20:00 至 2026-03-03 00:00 为威胁高发期，发生网络攻击，扫描等威胁行为，总计 6168 次。

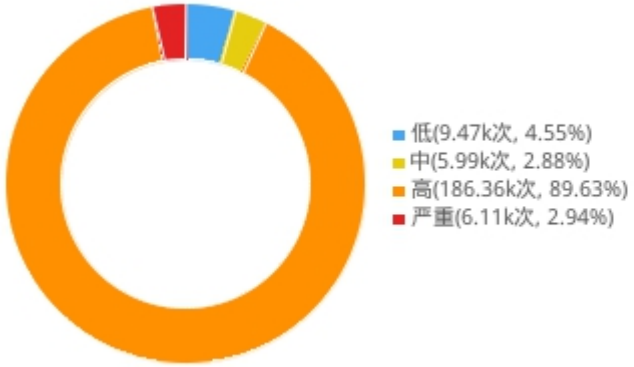
威胁趋势图



威胁类型分布

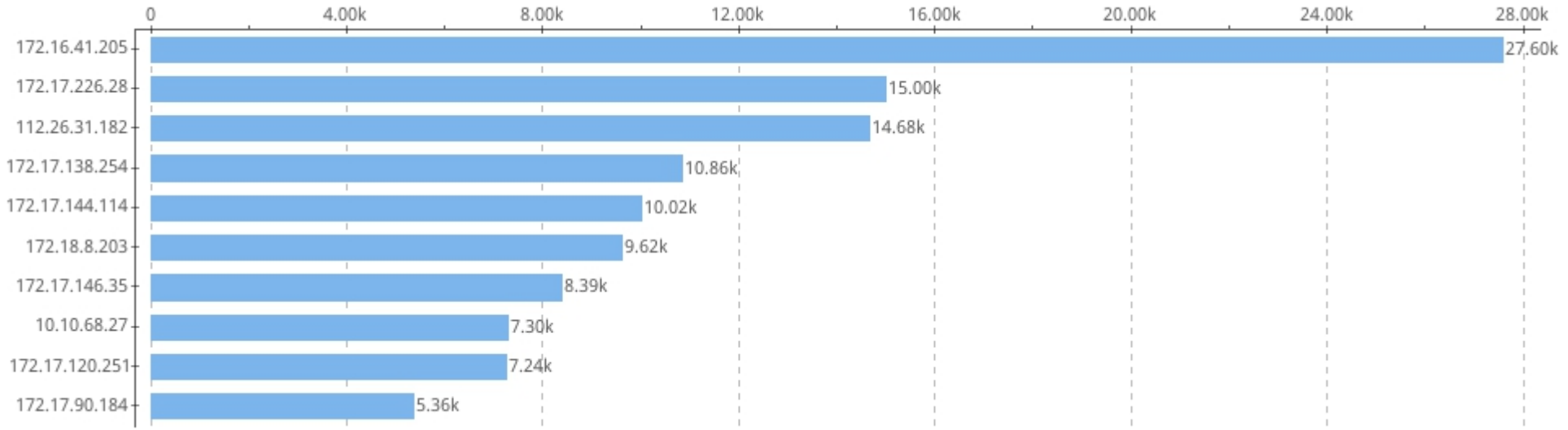


威胁严重程度分布

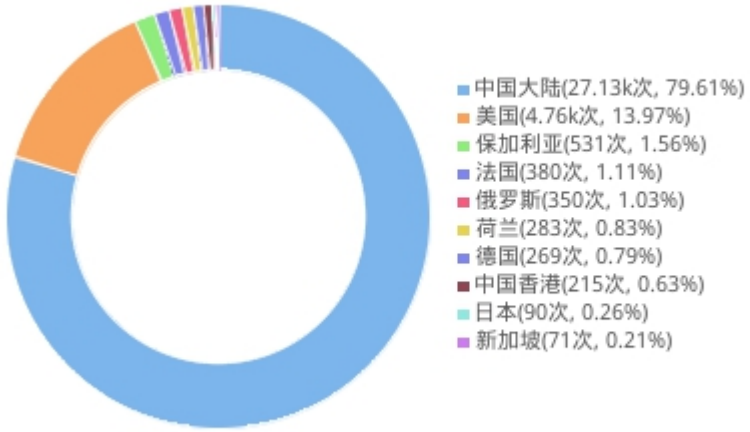


5. 网络风险威胁详情

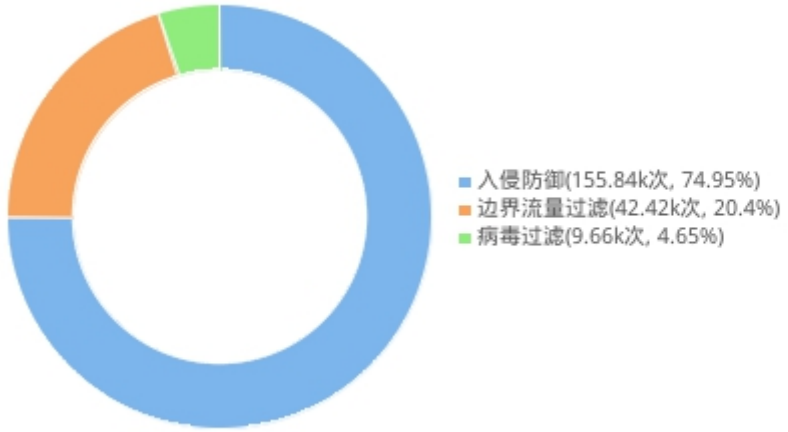
威胁攻击源排名



外部攻击地理分布



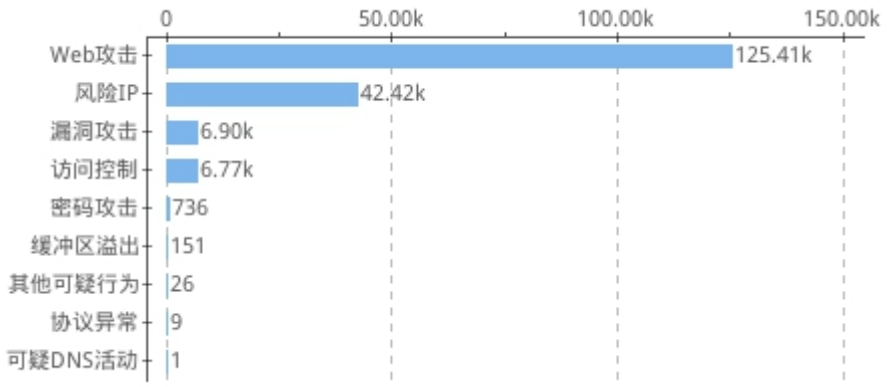
威胁检测引擎分布



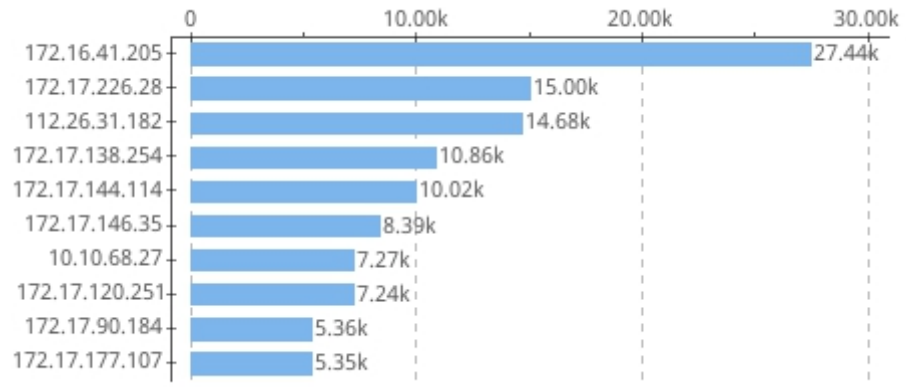
5. 网络风险威胁详情

发现 9 种网络攻击类型，其中 Web 攻击占比 68.75%，风险 IP 占比 23.25%，漏洞攻击占比 3.78%。

网络攻击类型排名

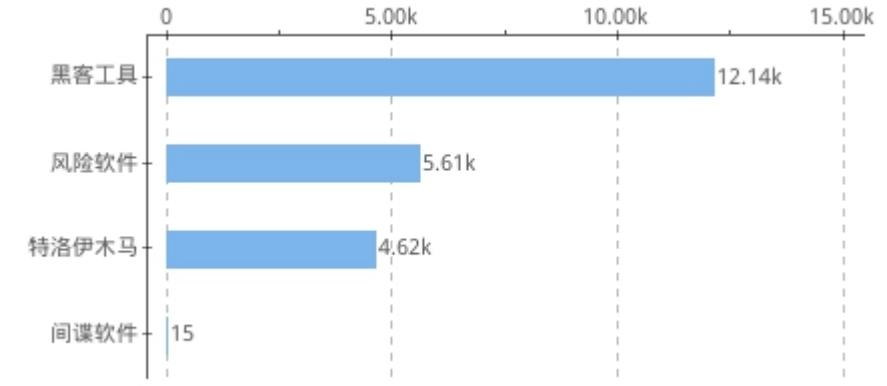


网络攻击类型攻击源排名

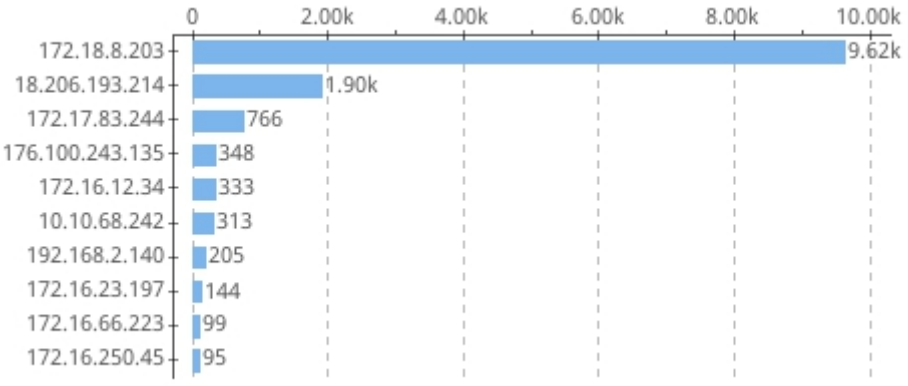


发现 4 种恶意软件类型，其中黑客工具占比 54.22%，风险软件占比 25.06%，特洛伊木马占比 20.65%。

恶意软件类型排名



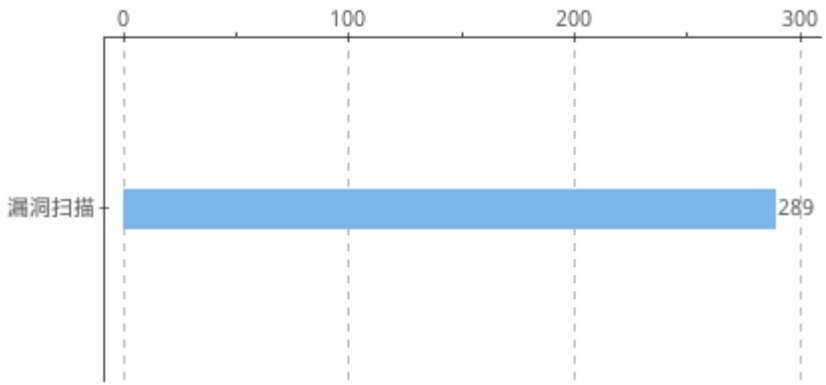
恶意软件类型攻击源排名



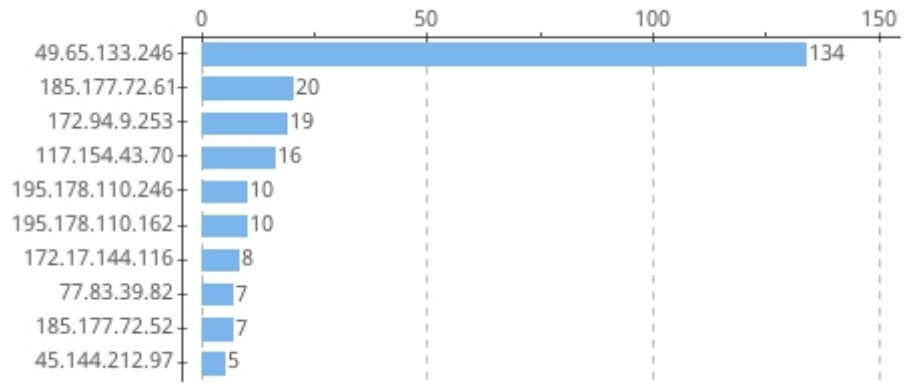
5. 网络风险威胁详情

发现 1 种扫描类型，其中漏洞扫描占比 100%。

扫描类型排名

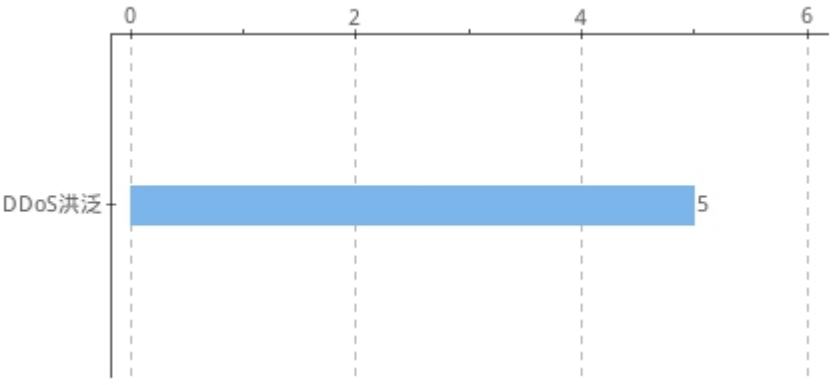


扫描类型攻击源排名

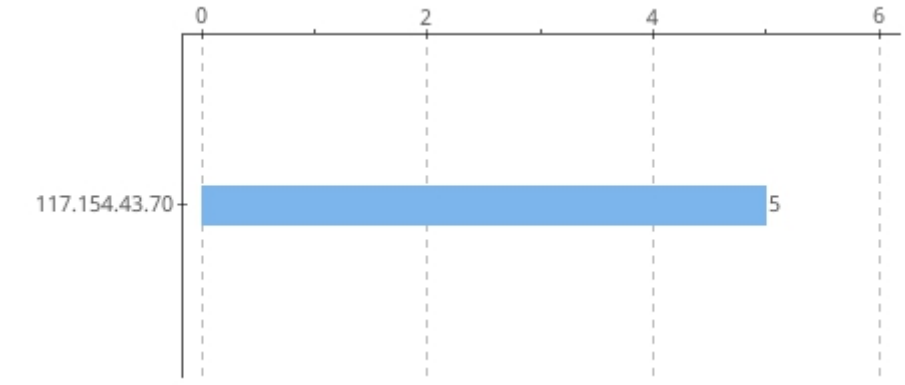


发现 1 种拒绝服务类型，其中 DDoS 洪泛占比 100%。

拒绝服务类型排名



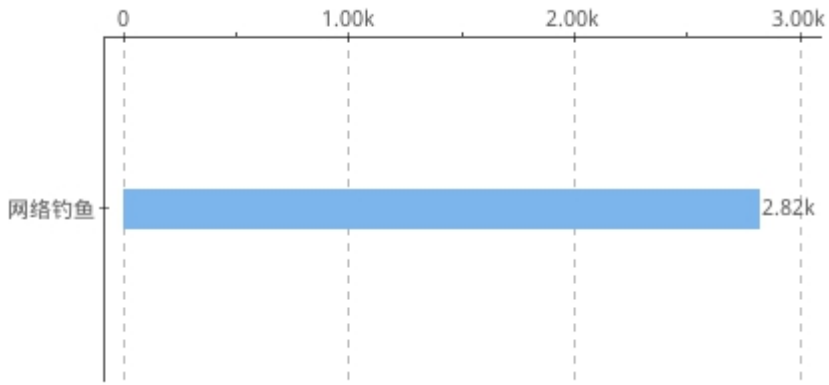
拒绝服务类型攻击源排名



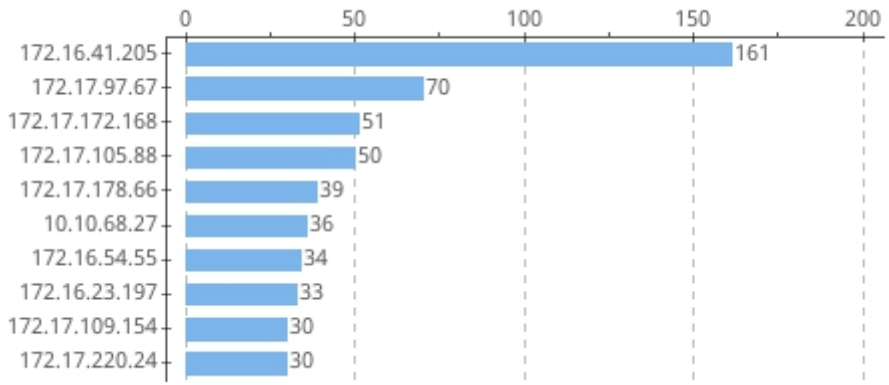
5. 网络风险威胁详情

发现 1 种网络钓鱼类型，其中网络钓鱼占比 100%。

钓鱼网站次数



钓鱼网站类型攻击源排名



未发现垃圾邮件。

垃圾邮件次数

没有数据

垃圾邮件类型攻击源排名

没有数据

6. 威胁说明

网络攻击

通过网络针对计算机软件系统、硬件系统、网络系统，以破坏信息系统的保密性、完整性、可用性、真实性和可控性为目的的行为，被称为网络攻击。网络攻击被分为：

WEB 攻击：随着 Web2.0、社交网络等一系列新型的互联网产品的诞生，基于 Web 环境的互联网应用越来越广泛，企业信息化的过程中各种应用都架设在 Web 平台上。Web 业务的迅速发展也引起黑客们的强烈关注，接踵而至的就是 Web 安全威胁的凸显，黑客利用网站操作系统的漏洞和 Web 服务程序的漏洞等得到 Web 服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据。此外，更为严重的是攻击者可以在网页中植入恶意代码，使得网站访问者受到侵害。常见的 Web 攻击有：1）SQL 注入攻击 2）跨站脚本攻击(XSS) 3）跨站请求伪造攻击(CSRF) 4）目录遍历攻击 5）网站信息泄露 6）网页挂马 7）服务器 Web Shell 挂马 8）Web 口令暴力破解 9）HTTP DDoS 攻击(CC 攻击) 10）网页篡改

密码攻击：攻击者攻击目标时常常把破译用户的口令作为攻击的开始。只要攻击者能猜测或者确定用户的口令，他就能获得机器或者网络的访问权，并能访问到用户能访问到的任何资源。如果这个用户有域管理员或 root 用户权限，这是极其危险的。常见的密码攻击有： 1）针对弱加密算法的攻击，例如 WEP WLAN 密码攻击 2）穷举法密码暴力破解 3）字典法密码暴力破解 4）社会工程学密码破解等

网络欺诈：这是一种严重的攻击形式，攻击者借用另外一台正常主机的信息，从而冒充另外一台机器与服务器通信。常见的 Spoofing 攻击有：1）IP Spoofing：行动产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。 2）ARP Spoofing：攻击者通过恶意 ARP 广播，将自己的 MAC 地址与被仿冒的主机 IP 地址进行绑定，以污染内网主机的 ARP 缓存。将所有到被仿冒主机的流量都牵引到攻击者主机。 3）DNS Spoofing：攻击者冒充域名服务器让目标主机把域名转换成错误 IP，其目的是让受害主机把通过域名查询到的 IP 地址设为攻击者所控制主机的 IP 地址。 4）WLAN Spoofing：攻击者通过仿冒受害者的无线 MAC 地址，从而代替受害者进行 WLAN 通信。

网络劫持：劫持攻击是一种网络攻击手段，攻击者可以通过破坏已建立的数据流而实现身份伪造并进行会话劫持。常见的劫持攻击有：1）TCP 劫持：通过侦测 TCP 序列号，通过模仿被劫持主机的 TCP/IP 序列号模仿被劫持主机的通信，而达到劫持的效果。 2）DNS 域名劫持：通过仿造 DNS 域名拥有者的身份信息，从而篡改域名信息、解析的地址，而达到盗窃域名所有权的后果。 3）基于代理的中间人攻击：通过使用代理服务器，在受害者的通信过程中可以监视或篡改受害者的通信信息。 4）HTTP 会话劫持：HTTP 会话信息通常使用 Cookie 存储。攻击者通过类似 XSS 攻击的手段，可以偷取用户的身份令牌。在身份令牌的有效期内，攻击者可以通过重放令牌的手段冒用受害者的身份。 劫持攻击的主要危害有： 1）嗅探敏感信息，例如受身份认证保护的涉密文件、信用卡密码等。 2）冒用管理员身份查看、修改系统关键信息，例如 passwd 文件等。

协议异常：目前多数网络攻击都是通过通信协议完成的，入侵引起的异常也表现为协议的异常，作为异常检测新的发展方向，协议异常检测对协议的正常数据建模，检测违反协议规定的行为和异常数据。

访问控制：访问控制是指用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术。该技术目的在于防止对任何资源进行未授权的访问，从而使计算机系统在合法的范围内使用。访问控制通常用于系统管理员控制用户对服务器、目录、文件等网络资源的访问。　　攻击者通常利用软件漏洞、弱口令探测、字典攻击、对认证服务器攻击等方式进行身份欺骗和绕过，从而可以访问受控制的资源。

恶意软件

恶意软件通常是指带有攻击意图的一段程序，主要包括：后门/木马，计算机病毒，计算机蠕虫，广告软件、黑客工具、间谍软件和风险软件。

扫描

扫描是一种是用扫描器完成的信息收集工作。在正式进行各种攻击行为之前，攻击者会采取各种手段，侦察对方的主机信息，以便决定使用何种最有效的方法达到自己的目的。攻击者通常使用扫描器来完成这个工作。扫描器是一类自动检测本地或远程主机安全弱点的程序，它能够快速的准确的发现扫描目标存在的漏洞并提供给使用者扫描结果。工作原理是扫描器向目标计算机发送数据包，然后根据对方反馈的信息来判断对方的操作系统类型、开发端口、提供的服务等敏感信息。

拒绝服务

DoS/DDoS 攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。这种攻击会导致资源的匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快都无法避免这种攻击带来的后果。　　常见的 DoS 攻击有：Smurf 攻击、TearDrop 攻击等等；常见的 DDoS 攻击有 TCP Syn Flood 攻击、TCP ACK Flood 攻击、ICMP Flood 攻击、HTTP CC 攻击、DNS 反射攻击等。　　要避免系统免受 DoS 攻击，网络管理员要积极谨慎地维护系统，确保无安全隐患和漏洞；而针对 DDOS 恶意攻击则需要安装防火墙等安全设备来过滤，同时应当定期查看安全设备的日志，及时发现对系统的安全威胁行为。

网络钓鱼

Phishing 与钓鱼的英语 fishing 发音相近，又名钓鱼式攻击。攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，骗取用户的私人信息。　　中国互联网络信息中心联合国家互联网应急中心发布的《中国网民网络信息安全状况调查报告》显示，近年来年有超过九成网民遇到过网络钓鱼。在遭遇过网络钓鱼事件的网民中，有超过 4000 万网民蒙受了经济损失，占网民总数 10%以上。网络钓鱼给网民造成的损失已超过 100 亿元人民币。

垃圾邮件

垃圾邮件一般具有批量发送的特征。其内容包括赚钱信息、成人广告、商业或个人网站广告、电子杂志、连环信等。垃圾邮件可以分为良性和恶性的。良性垃圾邮件是各种宣传广告等对收件人影响不大的信息邮件。恶性垃圾邮件是指具有破坏性的电子邮件。例如具有攻击性的广告：夸张不实，包括情色、钓鱼网站。有些垃圾邮件发送组织或是非法信息传播者，为了大面积散布信息，常采用多台机器同时巨量发送的方式攻击邮件服务器，造成邮件服务器大量带宽损失，并严重干扰邮件服务器进行正常的邮件递送工作。

7.网络安全防范提示与工作建议

为进一步筑牢校园网络安全防线，压实各部门网络安全主体责任，防范化解各类网络安全风险，针对本期监测发现的安全隐患与突出问题，特提出以下管理要求与防范提示：

（一）各部门网络安全管理工作要求

严格落实主体责任。严格遵循 **“谁主管谁负责、谁使用谁负责”** 的网络安全工作原则，各部门负责人为本单位网络安全第一责任人。针对 3 月通报的 3 起安全事件，涉事部门需限期完成整改闭环，其余部门需举一反三，全面开展本单位业务系统、网站、新媒体账号、数据资产的安全自查，及时消除存量风险隐患。

强化人员安全培训管理。定期组织本部门教职工、临聘人员、学生社团成员开展网络安全培训，重点覆盖钓鱼攻击防范、账号密码管理、数据安全保护、违规行为红线等内容，提升全员安全意识，杜绝因人为操作不当引发的安全事件。

规范账号与系统全生命周期管理。严格执行账号最小权限原则，及时停用、注销离职离岗人员的系统账号，严禁账号共享、转借行为；定期对本部门管理的业务系统、服务器开展漏洞扫描与补丁更新，关闭非必要端口与服务，严禁将校内业务系统、设备无防护直接暴露至公网。

健全应急处置与上报机制。各部门需明确网络安全应急联系人，发现系统异常、账号被盗、数据泄露、恶意攻击等安全事件时，第一时间对涉事设备做断网隔离处理，保留现场日志证据，并立即向学校网络信息中心上报，严禁擅自处置、瞒报漏报，避免威胁扩散与事态升级。

（二）通用网络安全防范小技巧

1. 账号与密码安全

办公系统、业务平台必须设置强密码，密码长度不低于 8 位，需同时包含大小写字母、数字与特殊字符，严禁使用生日、工号 / 学号、123456 等弱口令；

不同系统、平台需设置独立密码，避免 “一套密码全平台通用”，定期（每 3 个月）更换密码，不将密码记录在电脑桌面、便签等易泄露位置，严禁向他人共享、转借个人账号与密码。

2. 钓鱼攻击与诈骗防范

不点开陌生邮件、短信、微信群 / QQ 群内的不明链接与附件，不扫描来源不明的二维码，对索要账号密码、短信验证码、银行卡信息的内容，一律保持高度警惕；

所有校内通知、业务办理提醒，均以学校官方网站、官方公众号、正式公文渠道发布为准，收到可疑信息时，第一时间通过官方渠道核实，切勿轻信点击。

3. 终端与设备安全

办公电脑、个人终端需定期更新操作系统与杀毒软件，开启系统防火墙，定期全盘查杀病毒木马；

不私自安装盗版软件、破解工具、来源不明的程序，外接 U 盘、移动硬盘等存储设备时，务必先杀毒再打开访问；

严禁内网办公设备违规外联（如接入手机热点、公网 WiFi），校园内不连接名称与官方校园 WiFi 相似的不明热点，防范中间人攻击。

4. 数据与信息安全

不随意泄露、传播学生个人信息、教职工敏感信息、学校内部涉密文件与工作数据，敏感数据严禁存储在个人设备、公共云盘内；

严禁通过微信、QQ 等公共社交渠道传输涉密文件与敏感数据，内部工作群严格做好人员管理，不随意转发群内工作内容，杜绝数据泄露风险。

（三）后续工作安排

学校网络信息中心将持续开展校园网全流量监测、网络安全常态化巡检与专项漏洞扫描，定期组织网络安全培训与应急演练，为各部门提供技术支撑与安全指导。请各部门严格落实本通知要求，切实履行安全管理责任，共同维护校园网络环境安全稳定。