西安交通大学网络安全运行报告

报告日期：2026 年 10 月 12 日至 2026 年 10 月 20 日

1.网站防护：

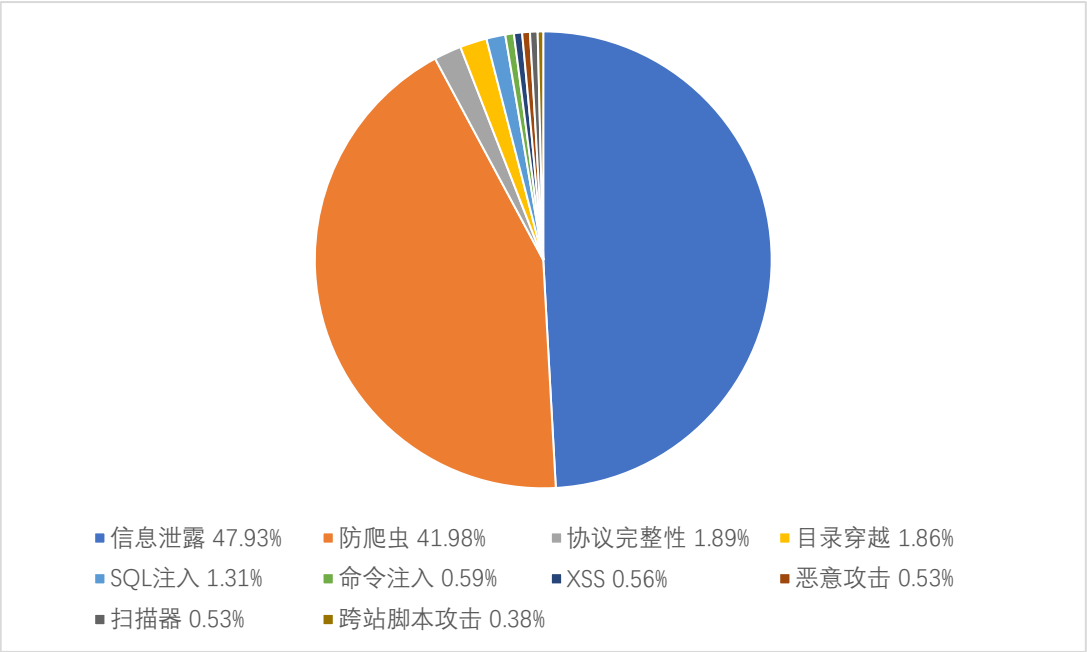
本周发现并阻止攻击行为 150 万 2 千余次，环比上周减少了 368 万 3 千余次，环比减少 71.03%，多为低危攻击行为，研究生院被频繁攻击。

日期	9 月 28 日-10 月 12 日	10 月 12 日-10 月 20 日
请求次数	**56403** 万次	**29661** 万次
被攻击次数	**518** 万次	**150** 万次
最多攻击类型	信息泄露	信息泄露
被攻击最多系统	研究生院	研究生院

攻击威胁来源地分布

本周发现的威胁来源境内主要是北京，网络攻击行为 49 万 5 千余次；境外主要是美国，网络攻击行为 6 万 4 千余次，其余地区攻击行为相对较少。

攻击类型分布

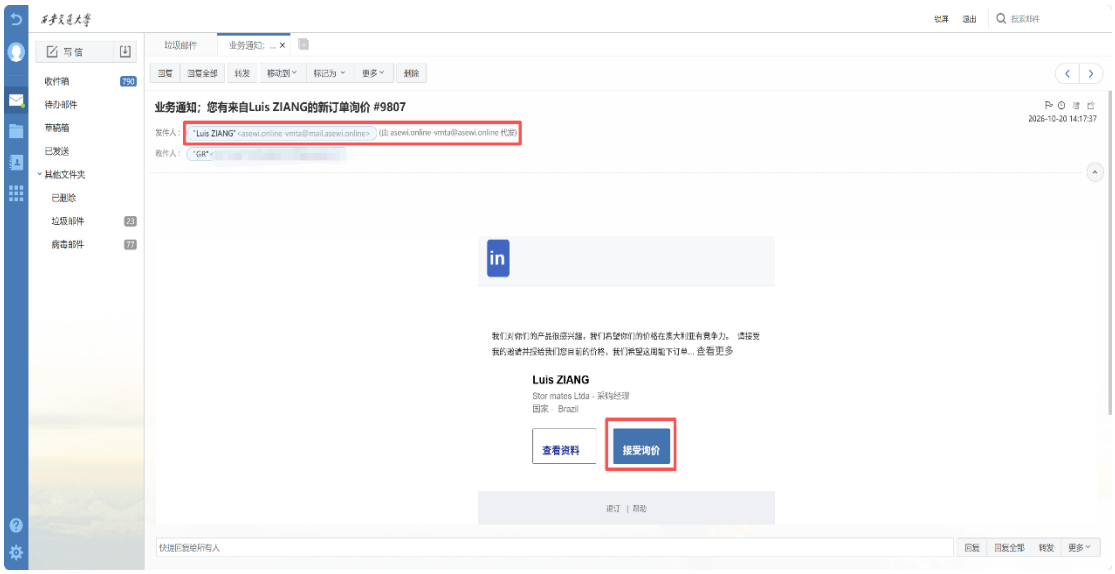


攻击类型分布

本周所受攻击中，低危攻击行为 83 万 9 千余次，信息泄露行为 71 万 9 千余次，相比上周低危攻击行为减少了 69 万 6 千余次，信息泄露行为相比上周减少了 95 万余次。

2. 邮件防护：

1. 本周钓鱼邮件有：①Luis ZIANG-业务通知



②ella-全球展台搭建



请各位用户不要打开以上邮件，特别是邮件附件，谨防造成数据加密或财产损失。

温馨提示：①不要从垃圾箱打开查看垃圾邮件；

②收到邮件时先查看发件人信息，确认是真的管理员 admin@xjtu.edu.cn 或其他官方账号，再阅读邮件内容，对于仿冒或代发的邮件直接删除，假冒发件人如下图所示：



③针对邮件内容索要账号密码、登录陌生链接、扫描二维码或下载附件等行为都存在安全风险，请谨慎操作。

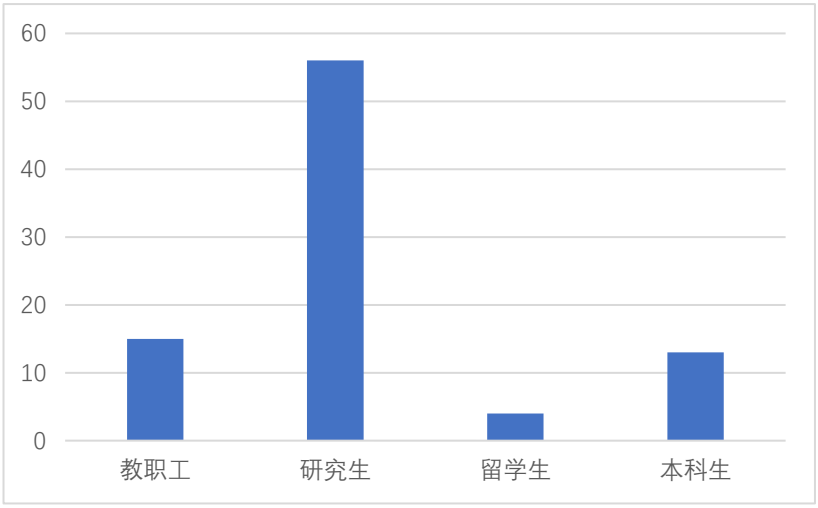
2.本周邮箱系统监控到多起暴力破解事件，暴力破解次数 35 起，涉及恶意外部攻击 IP 地址 19 个，对攻击较多 IP，我们采取措施，限制其对学校资源的访问。弱口令是暴力破解成功的主要诱因，一旦被破解将面临很严重的资产风险，导致我们邮箱里的重要文件受到损坏，可能导致不可逆的破坏和严重的经济损失。因此建议设置安全复杂的口令（8 字符以上且包含英文大小写+数字+符号的组合），同时一旦有暴露口令的风险一定要及时更换口令。

3.校内风险：

1.本周校内外通报事件 88 起，其中远控木马 84 起，挖矿木马 4 起，事件相关 IP 已通报封禁，并要求整改，具体数据如下：

风险类型	风险事件
远控木马	84
挖矿木马	4

2.从人员身份的角度分析，研究生占主体部分，具体数据如下：



人员类型分布

网络安全运行总结

1. 本周共发现攻击行为 150 万 2 千余次，同上周相比，攻击行为减少了 368 万 3 千余次，攻击类型以信息泄露为主。
2. 本周钓鱼邮件较少，各位用户也应注意防范，不要随意打开，以免造成损失；对于暴力破解事件需加强巡查，对攻击行为及时处理；邮箱应启用强口令，提高防破解能力。
3. 本周校内风险事件较多，攻击类型以远控木马为主，涉及人员以研究生为主，应加大对研究生网络安全相关知识的普及和教育工作。