安徽文达信息工程学院
网络信息中心
网络安全月报（六月）

报告类型： 网络安全

报告周期： 2026-06-01 09:08:00 - 2026-06-30 08:18:00

报表项内容：

一、本月网络安全总体概况

二、互联网数字资产与暴露面风险

三、漏洞与脆弱性风险

四、内外网威胁事件分析

五、整改及安全建设建议

六、下月重点工作提示

一、本月安全总体概况

6 月份平台共监测 18006 个 IP，产生 145 万 + 安全告警，识别 910 个存在高风险行为 IP；平台未启用旁路阻断自动编排功能，全部威胁仅告警记录，无自动封堵处置，威胁处置全部依赖人工研判操作。

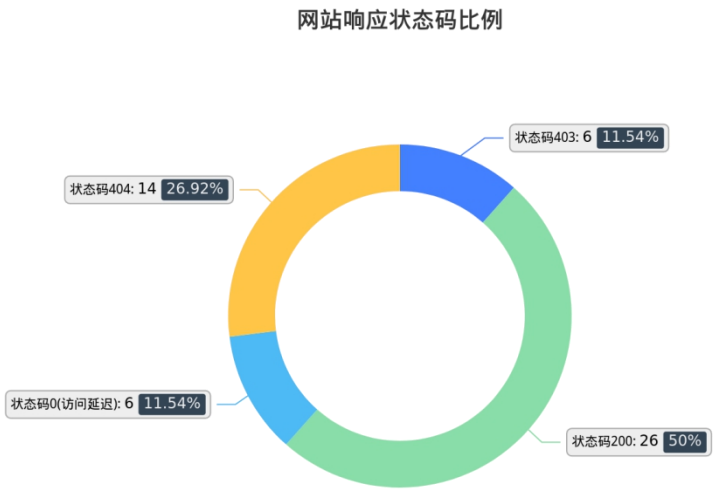
本月未发生重大网络安全事件，但校内安全风险压力突出：内网共监测 895 台病毒木马非法外联主机，5 台可疑失陷主机，大量终端感染 xred 蠕虫、银狐远控、zegost 后门等恶意程序，内网横向扩散风险高；互联网侧共监测存活 Web 资产 46 个，发现 26 个对公网开放的后台登录入口，3 个未做访问权限控制的 Swagger 敏感 API 接口，32 个搭载 Struts2、Tomcat 等高风险易危组件网站；互联网 Web 系统累计发现高危漏洞 2 个，中危漏洞 25 个，存在网站敏感文件泄露、页面植入黑链、业务系统 502 超时可用性故障等问题；主机侧累计遗留大量未整改漏洞，存在 FTP 弱口令账号风险；主机 Agent 部署覆盖率为 0，缺少终端主机安全监测能力，主机测绘、主机脆弱性扫描任务本月未执行，安全监测存在盲区。

整体来看，学校当前主要风险集中在互联网暴露面管控不足、Web 系统漏洞隐患、内网终端病毒蠕虫大规模感染、安全监测防护能力缺失、漏洞闭环整改机制不完善五大方面，需要落实专项整改，降低网络安全风险。

二、互联网数字资产与暴露面风险

2.1 互联网资产概览

本月监测存活互联网 Web 资产 46 个，本期无新增 Web 资产；未监测到存活互联网主机 IP 及互联网端口资产；未发现有效 ICP 备案、公众号、小程序、APP 等外部数字资产。 网站响应状态码统计：200 正常访问占 50%；404 占 26.92%；403 占 11.54%；访问超时 0 占 11.54%，部分业务存在访问异常情况。



2.2 高风险暴露资产

1. 登录入口：共监测 26 个网站后台登录入口直接暴露互联网，包含邮箱管理员登录、报名系统后台等，后台直接对公网开放，易遭受暴力破解攻击。
2. 敏感 API 地址：监测 3 个公网可直接访问 Swagger-ui 接口文档，无鉴权控制，攻击者可获取接口参数，开展未授权访问测试。
3. 易危组件：32 个网站使用 Struts2、Tomcat8.5 系列、CKEditor 等漏洞频发组件，学校官网、报名系统、督导评教、邮箱系统均受影响，存在被漏洞利用入侵风险。
4. 其它暴露风险：本期未发现公网泄露敏感代码片段、敏感文档、邮箱信息。

三、漏洞与脆弱性风险

3.1 互联网 Web 漏洞风险

本月共监测互联网 Web 高危漏洞 2 个、中危漏洞 25 个，主要漏洞类型包含跨站脚本 XSS、CORS 跨域配置错误、TLS1.0/TLS1.1 老旧协议启用、SSL 弱密码、Webpack 源码泄露、JavaScript 库漏洞、明文传输用户凭证等。 主要受影响系统：学校官方网站、文达邮箱系统、学生综合管理服务平台、督导评教系统。官网存在老旧 TLS 协议、跨站脚本风险；邮箱系统存在 CORS 配置错误、JS 组件漏洞；综合管理平台存在明文传输凭证、报错信息泄露等风险。

3.2 内网主机脆弱性风险

主机扫描任务本期未执行，历史累计未整改漏洞数量较大： 优先修复漏洞：351 个 次要修复漏洞：1658 个 按需修复漏洞：619 个 弱口令：1 个

重点风险：内网存在 root/root 的 FTP 弱口令账号，极易被攻击者爆破入侵；大量服务器存在 Apache、Tomcat、OpenSSH、Oracle 数据库、VMware ESXi 等高危 CVE 漏洞，部分漏洞支持远程利用。

3.3 网站安全监测风险

本月网站安全监测结果：敏感词 0 条；敏感文件 42 个；黑链 / 挂马 11 条；网站篡改 0 条；可用性故障 27 起。

1. 敏感文件泄露：官网存在大量对外公开 Excel、PDF 文档，文档内包含手机号、明文密码、标注“机密”的资料，造成个人信息及内部资料泄露。
2. 黑链植入：网站 js 脚本文件被植入非法赌博、色情类外部跳转黑链，主要集中在官网静态 js 资源，会造成学校网站公信力受损，搜索引擎降权。

3. 业务可用性故障：学生综合管理平台、学校官网、邮箱系统多次出现 502 Bad Gateway、访问超时，业务稳定性不足，影响师生正常使用。

四、内外网威胁事件分析

4.1 内网安全事件

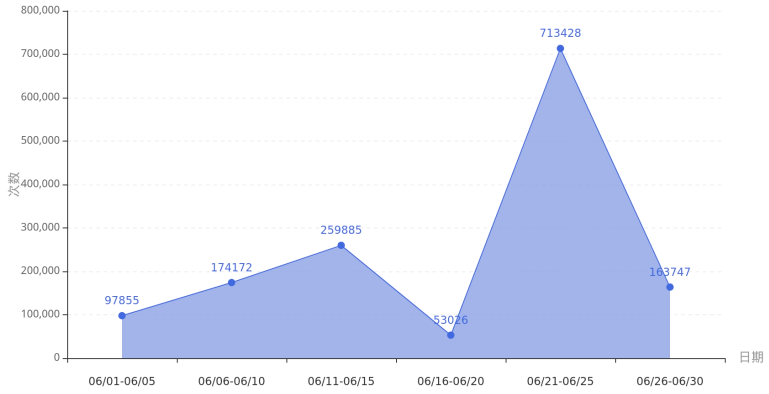
1. 可疑失陷主机：监测 5 台内网主机流量行为异常，判定疑似失陷，存在对外攻击行为，需要开展隔离、取证、全盘查杀。
2. 非法外联中毒主机：共 895 台主机病毒木马外联告警，大量终端感染 xred 蠕虫家族、银狐远控、zegost 后门、phonzy 远控木马，持续请求外网恶意域名、C2 服务器。蠕虫病毒在内网扩散，若不处置会造成批量终端失陷，存在内网横向渗透、信息窃取风险。

现状：全部告警主机处置状态均为未处置，缺少 Agent，无法进行主机层面深度检测，只能依靠流量告警识别风险。

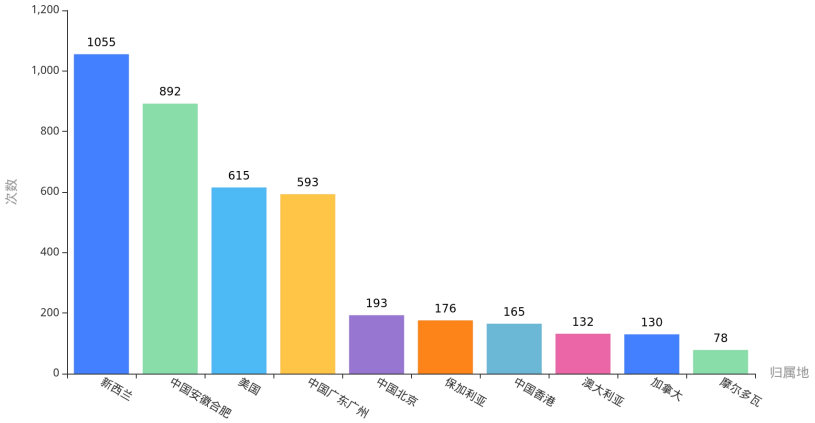
4.2 外网威胁告警

本月共捕获外网攻击 IP155 个，其中高风险 IP10 个、中风险 IP8 个、低风险 IP137 个；0 个 IP 自动阻断，全部依靠人工处置。攻击来源包含境外以及国内北京、广州、合肥等地区 IP。 攻击行为统计：病毒木马外联占比最高，其次为口令暴力破解、端口扫描、可疑网络行为；平台未开启自动阻断编排，攻击源仅记录日志，攻击源可以持续扫描探测校内 Web 与网络资产。

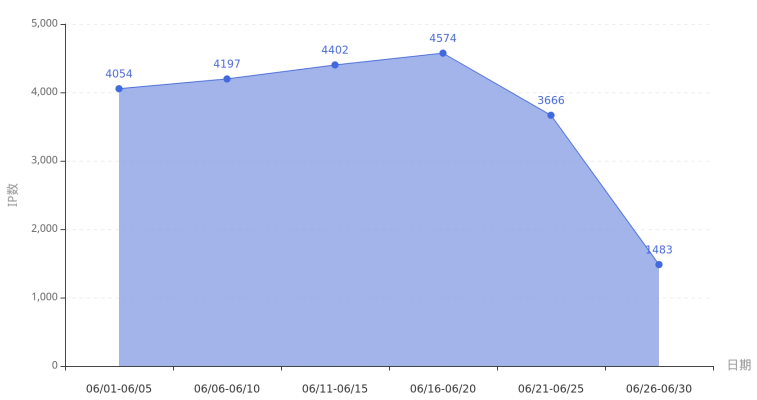
攻击次数趋势



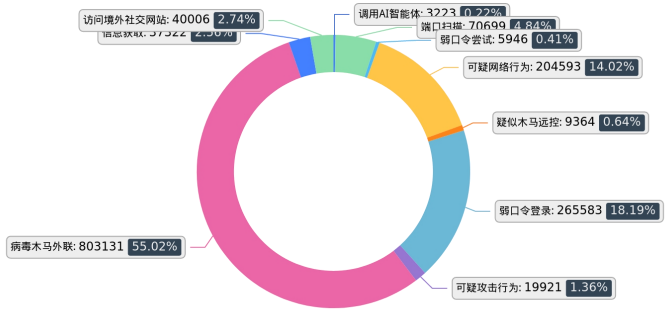
攻击归属地TOP10



攻击IP数趋势



攻击类型统计



4.3 安全运营任务执行现状

主机资产测绘：本期未执行 网站资产测绘：执行 1 个任务，探测 1 个 web 主机脆弱性扫描：本期未执行 网站脆弱性扫描：执行 7 个任务，扫描 4 个网站 网站黑链 / 敏感文件监测：下发任务监测 4 个网站 蜜罐部署：0 个蜜罐 IP，未启动 主机 Agent：0 台服务器 / 终端安装，在线 Agent 为 0

核心短板：主机测绘、主机漏洞扫描任务缺失，Agent 零部署，内网服务器、终端没有主机层面安全检测能力，大量风险只能靠流量被动发现，无法做主机基线、病毒查杀、异常行为监测。

五、整改及安全建设建议

5.4 漏洞闭环与防护策略

1. 建立漏洞分级整改台账，压实整改责任主体 针对平台扫描输出的优先修复漏洞 351 个、次要修复漏洞 1658 个、按需修复漏洞 619 个以及现存 FTP 弱口令问题，建立完整漏洞整改台账。台账需要包含漏洞编号、受影响资产 IP/URL、漏洞风险等级、漏洞描述、影响业务系统、责任运维部门、整改时限、整改措施、复测结果等关键字段。按照“高危优先、业务优先”原则划分处置优先级，将 Apache、Tomcat、OpenSSH、Oracle 数据库、VMware ESXi 等服务器高危可远程利用漏洞列为第一优先级；对学校官网、报名系统、学生综合管理平台、邮箱系统等关键业务资产漏洞优先处置。明确各业务系统运维负责人，落实“谁主管、谁运维、谁负责”，杜绝漏洞长期搁置无人处置的现象。针对老旧业务系统无法直接打补丁升级的，需要书面记录系统现状，明确对应的临时补偿防护手段，严禁仅登记漏洞而不采取任何防护措施。结合 6 月报表现状，尽快补做主机资产测绘、主机脆弱性扫描任务，补齐主机侧漏洞数据，完善台账信息。
2. 落实漏洞整改- 复测闭环管理，杜绝虚假整改 严格执行“漏洞发现→下发整改通知→实施修复→漏洞复测→闭环归档”全流程闭环机制。漏洞修复完成后，不能仅凭运维人员口头确认完成修复，需要依托安全平台重新开展扫描复测，复测确认漏洞消除后，才允许标记闭环。复测仍存在漏洞

的资产，执行二次督办，约谈对应运维负责人，深度分析无法整改的根因。 针对因业务兼容性、系统停止维护等客观约束不能直接修复的漏洞，不能直接忽略放过，必须落实补偿防护手段，包括配置防火墙访问策略限制访问源 IP、配置 WAF 防护规则、网络逻辑隔离受影响资产；同步完成风险评估，留存风险豁免审批文档，定期复评风险，一旦条件具备立刻正式修复。 优先处置本次发现的 FTP root/root 弱口令，修改高强度密码，严格限制 FTP 访问源地址，整改完成后开展账号安全专项复测，避免弱口令复现。针对互联网 Web 系统的 XSS、CORS 配置错误、老旧 TLS 协议、明文凭证传输等 Web 漏洞，督促网站运维完成配置整改，停用 TLS1.0、TLS1.1，强制启用 TLS1.2 及以上安全协议。

3. 启用平台旁路阻断编排功能，强化对外攻击自动防御能力 6 月监测到 155 个外网风险攻击 IP，包含 10 个高风险 IP，但平台尚未启用旁路自动阻断编排，所有恶意 IP 仅留存告警日志，完全依赖人工研判处置，响应滞后，容易错过攻击处置窗口期。建议尽快完成旁路阻断编排配置上线，配置自动化阻断策略：对暴力破解、漏洞探测、恶意外联、Web 攻击等高风险行为源 IP 自动拦截；同步配置阻断白名单，保障校内、合作单位合法业务 IP 不会被误封；留存完整阻断审计日志，按月复盘攻击 IP，统计攻击来源、攻击类型趋势。同时保留人工处置流程，安全运维人员每日巡检平台外网告警，对确认恶意 IP 执行手动拉黑，弥补自动策略覆盖不全的缺陷。
4. 常态化开展漏洞扫描与安全检测工作 改变当前主机漏扫任务长期不执行的现状，建立常态化扫描机制：主机脆弱性扫描至少每月执行一次；网站脆弱性扫描每两周执行一次；业务系统上线、版本迭代、配置变更后执行临时专项扫描，防止变更引入新安全漏洞。利用平台资产测绘能力及时识别新增互联网暴露资产，做到新增资产即扫描。 分步推进主机 Agent 部署工作，解决当前 Agent 在线数量为 0 的短板，优先覆盖核心业务服务器，逐步扩展到重点办公终端，补齐主机层面的监测能力。定期核查扫描任务运行状态，及时处理任务失效、任务未正常调度的问题，避免扫描任务失效长期无人知晓。
5. 漏洞数据汇总分析，驱动系统架构优化 按月度对全部漏洞数据开展统计分析，梳理高频出现的漏洞类型。针对反复出现的同类漏洞，溯源产生根源，区分是开发编码缺陷、组件版本管控缺失、还是上线流程缺少安全检查。将漏洞统计分析结果同步开发、运维部门，推动安全前置到系统开发、版本上线环节，从源头降低漏洞产生，而不是仅依靠事后扫描修复。结合本月大量 Struts2 组件风险，推动老旧组件梳理替换工作。

5.5 安全管理建议

1. 分层分类开展全员网络安全宣传与技能培训 面向不同对象开展差异化安全教育。面向全体师生，重点开展终端安全意识培训，讲解 xred 蠕虫、银狐远控、钓鱼邮件、恶意链接识别防范；教育师生不要运行来源不明软件，及时更新系统补丁、杀毒病毒库，降低终端中毒概率，从源头减少内网非法外联事件。 面向各业务系统运维人员，开展专项安全运维培训，培训互联网暴露面收敛、漏洞修复规范、Web 网站加固、恶意事件处置、日志审计实操；重点结合本月发生的内网大规模蠕虫感染、网站黑链植入、敏感文件泄露等真实风险开展案例警示教育，提升运维实操能力。

面向信息化安全管理人员，重点培训威胁告警研判、安全平台操作、网络安全事件应急处置流程，提升整体安全运营能力。培训留存签到、课件、培训记录归档。

2. 落实内网网络分区隔离，遏制病毒横向扩散风险 本月监测 895 台非法外联中毒主机，5 台疑似失陷主机，内网蠕虫病毒传播风险极高。需要推进内网安全域划分，划分为办公终端域、学生终端域、业务服务器域、核心数据库域，域之间部署访问控制策略，严格跨域访问。办公、学生终端域禁止直接访问核心业务服务器；服务器之间遵循最小权限开放端口，阻断蠕虫木马横向传播路径。 建立中毒主机快速隔离机制：平台监测到恶意外联、失陷告警后，将对应主机隔离至隔离 VLAN，禁止访问内网其他业务，完成全盘杀毒、风险验证确认安全后，再恢复网络权限。配置边界 DNS 过滤、黑名单，拦截终端访问外网恶意域名、C2 服务器，阻断木马外联通道。
3. 完善数据备份与网络安全应急处置预案，定期组织演练 梳理官网、报名系统、学生综合管理平台、邮箱等核心业务系统，落实本地 + 异地备份策略，执行全量 + 增量备份，定期验证备份数据可恢复性，应对网站篡改、病毒加密、系统故障业务瘫痪风险。 修订学校网络安全应急预案，明确事件分级、告警研判流程、处置分工、上报流程、溯源取证、事后复盘流程，针对网站黑链篡改、蠕虫病毒大规模爆发、服务器被入侵、敏感信息泄露等典型场景编制处置操作手册。结合 6 月真实风险场景开展应急演练，模拟内网大规模蠕虫爆发、网站植入黑链、敏感文件泄露等场景，检验运维处置能力；演练完成后复盘优化预案处置流程。严格落实网络安全事件上报制度，发生重大网络安全事件按照上级主管部门要求及时上报。
4. 强化系统上线变更安全管控，把好安全准入关口 建立系统上线、版本变更安全检查机制。新业务上线前必须完成安全测评，开展漏洞扫描、互联网暴露面核查，禁止高危漏洞、后台管理接口直接暴露公网的系统直接上线。系统版本升级、配置修改完成后开展安全复核，避免变更引入新风险。新增 Web 资产第一时间纳入安全监测范围。 强化外包开发运维管理，对外包建设运维的网站业务系统明确网络安全责任，要求外包遵循安全开发规范，交付系统完成安全自查；定期对外包运维网站开展安全抽查，防范外包运维不当带来漏洞、黑链、信息泄露问题。结合 6 月监测 26 个后台登录入口直接暴露互联网，尽快开展后台访问收敛，后台限制内网 / IP 白名单访问，远程运维优先使用 VPN、堡垒机。下线不需要对外公开的 Swagger 接口，确需使用必须增加鉴权控制，禁止公网直接访问。
5. 健全常态化巡检考核机制，推动安全风险闭环落地 执行月度网络安全风险巡检，依托安全平台月报跟踪上月风险整改情况，对逾期未整改风险持续督办。将网络安全风险整改落实情况纳入运维岗位绩效考核，提升运维人员安全重视程度。持续开展全量资产梳理，摸清互联网 Web、内网服务器、终端资产台账，消除资产“看不见、管不到”的管理盲区。持续优化平台告警规则，过滤无效告警，提升安全人员告警研判效率。按月向各业务主管部门通报本部门业务系统安全风险，压实业务部门主体责任，形成“监测- 通报- 整改- 复测- 考核”常态化安全管理闭环。
6. 推进安全能力补齐建设 当前主机 Agent 部署数量为 0，主机测绘、主机漏洞扫描任务缺失，主机安全监测存在明显短板。分步推进服务器、重点终端 Agent 部署，实现主机日志采集、异常行为监测、病毒查杀、基线核查能力，改变只依靠外部流量扫描的被动防御模式。 评估现有 WAF、堡垒机设备使用效果；对公网暴露业务完善 WAF 防护规则；推广堡垒机开展服务器运维，减少直接对公网开放管理端口与后台。针对大量 Struts2

易危组件，梳理业务系统清单，制定组件升级或虚拟补丁防护方案。针对官网等网站存在的敏感文件泄露、JS 黑链问题，开展专项清理，删除公网敏感文档，清除页面 JS 黑链代码，排查是否存在 Webshell 入侵痕迹。针对学生综合管理平台、邮箱系统频繁 502、访问超时问题，排查服务器资源瓶颈，优化业务保障业务可用性。

六、下月重点工作提示

1. 优先处置内网 895 台非法外联中毒主机、5 台可疑失陷主机，分批隔离查杀，遏制蠕虫病毒在内网继续扩散；
2. 开展互联网暴露面专项收敛：26 个后台登录入口、3 个 Swagger API 接口整改管控；清理网站敏感泄露文件、清除网站黑链代码；
3. 补全主机测绘、主机脆弱性扫描任务，启动主机 Agent 部署试点；
4. 完成旁路阻断编排功能配置启用；
5. 开展高危漏洞、FTP 弱口令专项整改，完成复测闭环；
6. 完善内网安全域规划，推进网络隔离策略落地。