



安徽文达信息工程学院
网络信息中心
网络安全月报（五月）

报告类型： 网络安全

报告周期： 2026-05-01 09:08:00 - 2026-05-30 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、安全运营与内外网威胁态势

四、主要风险汇总

五、整改及安全建设建议

一、本月网络安全总体概况

本月通过平台完成互联网暴露面测绘、安全运营威胁监测、漏洞脆弱性扫描、网站安全监测等工作。本月累计检测 20118 个 IP，产生 111 万 + 条安全告警，研判识别 1255 个存在高风险行为 IP；平台未开启旁路自动阻断功能，威胁未实现自动封堵。

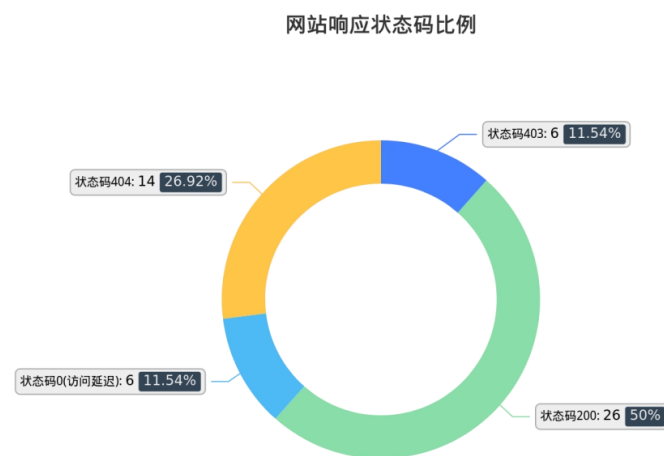
整体风险情况：外网 Web 资产存在较多暴露风险，后台登录入口、高危组件对外暴露，网站存在高危、中危漏洞；网站出现敏感文件泄露、黑链植入、可用性故障；内网环境存在大量非法外联主机以及可疑失陷主机，病毒木马感染现象突出，大量主机漏洞长期未整改，整体网络安全风险较高，需加快风险处置闭环。本月未发生重大网络安全事件。

二、互联网数字资产与暴露面风险

2.1 互联网数字资产盘点

1. Web 资产：存活互联网 Web 资产 46 个，本期新增 1 个。
2. 互联网主机、端口资产：未监测到存活互联网 IP 与互联网端口资产。
3. 其他资产：未发现 ICP 备案、企业信息、APP、微信公众号、服务号、小程序资产。

网站响应状态码统计：状态码 200 占 50%，状态码 404 占 26.92%，状态码 403 占 11.54%，访问延迟占 11.54%，部分网站访问异常。



2.2 高风险暴露资产（收敛建议项）

1.登录入口：共监测登录入口 26 个，本期新增 2 个，全部为网站后台登录入口。邮箱登录、综合管理平台、报名系统后台直接对外开放互联网。

建议：后台管理系统禁止直接对公网开放，配置 IP 白名单，仅允许校内可信地址访问。

2. 敏感 API 地址：识别 3 个 Swagger 接口文档地址，无新增。Swagger 接口容易产生未授权访问，需要核查接口访问权限控制有效性。

3. 易危组件网站：32 个网站存在 Struts2、Tomcat、CKEditor 等高风险组件，本期新增 1 个。Struts2 历史漏洞多，容易被攻击者利用获取服务器权限，需升级组件补丁。

4. 未检出敏感代码片段、敏感文档、邮箱信息。

2.3 互联网漏洞风险

- Web 漏洞：高危漏洞 1 个，中危漏洞 23 个。主要包含跨站脚本攻击、TLS1.0/1.1 老旧协议启用、SSL 弱密码、Sweet32 攻击、JavaScript 库漏洞、Webpack 源码泄露、CORS 跨域配置错误等问题。
- 互联网主机：未检测到可利用主机高危漏洞；无弱口令告警。

2.4 互联网网站监测风险

序号	监测项	结果概述与建议
1	网站风险监测	概述： 累计共发现 0 个敏感词，24 个敏感文件，11 个黑链，0 个网站篡改，25 个网站可用性故障。

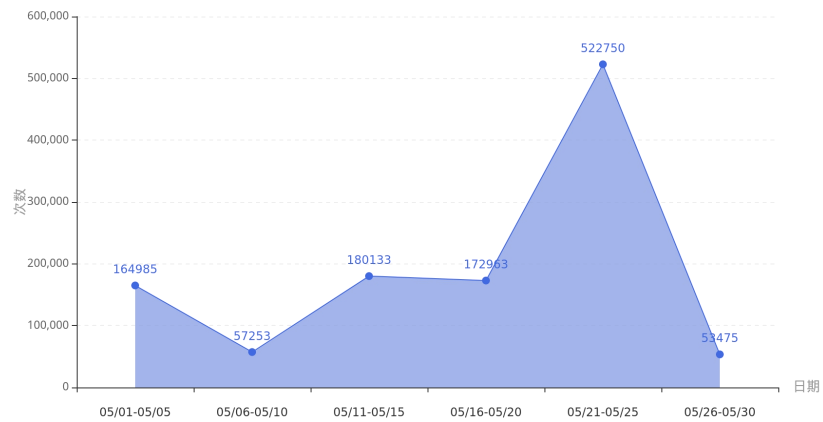
风险说明：敏感文件泄露造成师生个人信息外泄；黑链会损害学校公信力，搜索引擎降权；频繁可用性故障影响师生正常访问业务系统。

三、安全运营与内外网威胁态势

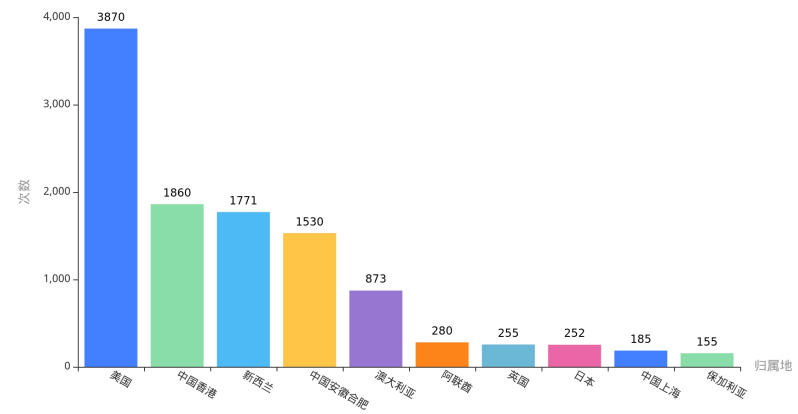
3.1 外部攻击态势

本月共计监测外网风险 IP138 个：高风险 IP2 个、中风险 IP3 个、低风险 IP133 个，全部未处置，无自动阻断。
攻击来源地 TOP：美国、中国香港、新西兰、安徽合肥等地区。
攻击类型占比：病毒木马外联占比最高 51.94%，其次可疑网络行为 20.18%，弱口令登录 14.41%。
攻击峰值：5 月 21- 25 日攻击量达到峰值 522750 次，外部攻击强度波动明显。

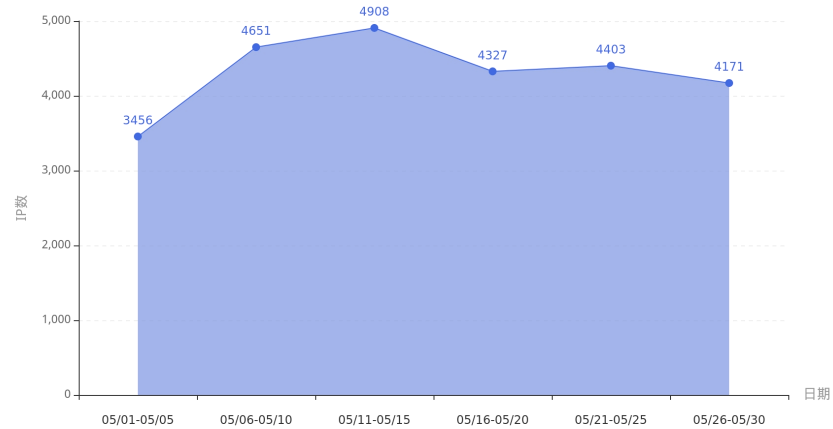
攻击次数趋势



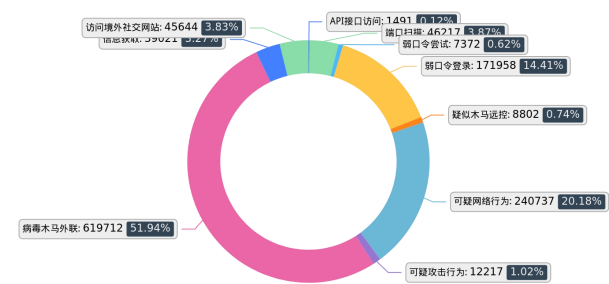
攻击归属地TOP10



攻击IP数趋势



攻击类型统计



3.2 内网安全事件（重点风险）

1. 可疑失陷主机：9 台，内网主机出现异常攻击行为，标记为流量高风险源 IP，建议对主机进行全盘查杀，排查是否被入侵控制。
2. 非法外联主机：1244 台，大量内网主机向外网恶意域名、恶意 IP 建立连接，主要感染 xred 家族蠕虫，同时存在 phonzy、银狐、Zbot、zegost 后门、挖矿访问等木马家族，疑似大规模中毒，风险突出。

说明：大量主机发生病毒木马外联，说明内网终端防护薄弱，蠕虫病毒在内网扩散，若不处置，攻击者可横向渗透到服务器区域。

3.3 资产脆弱性情况

1. 主机漏洞：累计未整改优先修复漏洞 351 个，次要修复漏洞 1658 个，按需修复漏洞 619 个；未整改弱口令 1 条（FTP root/root），所有漏洞本期整改数量为 0。主要漏洞包含 Apache、Tomcat、OpenSSH、Oracle 数据库、VMware 等组件漏洞。
2. 网站脆弱性：累计未整改高危漏洞 1 个，中危漏洞 8 个。
3. 任务执行情况：网站漏洞扫描执行 8 次任务，扫描 4 个网站；网站监测下发黑链、敏感文件监测任务；未执行主机漏洞扫描；平台 Agent 部署数量为 0，缺少终端监测能力。

3.4 资产变化统计

- 主机资产：本月无新增、无下线主机资产。
- 网站资产：外网网站资产新增 1 个；访问异常下线 9 个网站（外网 6 个，内网 3 个）。

四、主要风险汇总

- 1.互联网暴露面风险突出：大量业务后台登录接口、Swagger API、Struts2 高危组件直接暴露公网，攻击者可直接发起攻击。
- 2.Web 安全问题集中：老旧 TLS 协议、弱加密、XSS 跨站、跨域配置错误；网站存在敏感文件泄露、黑链植入、业务系统频繁可用性故障。
- 3.内网终端大规模中毒：一千余台主机存在病毒木马非法外联，蠕虫病毒扩散，9 台疑似失陷主机，内网横向渗透风险高。
- 4.漏洞整改工作停滞：几百个高危优先修复漏洞、弱口令长期未整改，没有闭环；无主机 Agent，缺少终端安全监测手段。
- 5.安全防护能力不足：未启用旁路自动阻断，外部攻击 IP 无法自动封堵，告警处置全部依赖人工。

五、整改及安全建设建议

5.1 互联网暴露面收敛

- 1.后台管理系统：邮箱、报名系统、综合管理平台后台禁止对公网开放，配置 IP 白名单，仅校内访问，确需远程管理使用 VPN / 堡垒机。
- 2.下线不必要 Swagger 接口文档，如业务必须使用，增加登录鉴权，禁止公网直接访问。
- 3.对 Struts2、Tomcat 等易危组件进行版本升级，无法升级的旧系统部署 WAF 虚拟补丁防护。

5.2 网站安全加固

- 1.清理网站敏感文件，对包含手机号、密码、绝密标记的文档，删除或做脱敏处理，避免公开泄露。
- 2.清除网站页面、JS 脚本内的黑链恶意代码，排查网站是否被 Webshell 入侵，加强网站定期巡检。
- 3.升级网站加密套件，停用 TLS1.0、TLS1.1，启用 TLS1.2 及以上安全协议，修复跨站脚本、CORS 配置错误等 Web 漏洞。
- 4.排查 502、访问超时业务系统，优化服务器资源，保障业务可用性。

5.3 内网风险处置（最高优先级）

- 1.对 1244 台非法外联主机分批排查，进行全盘杀毒、查杀蠕虫病毒；重点清理 xred 蠕虫、银狐远控、各类后门木马。

2. 对 9 台可疑失陷主机隔离处置，取证排查入侵痕迹，确认是否被攻击者控制。
3. 排查 FTP 弱口令账号 root/root，立即修改高强度密码，限制 FTP 访问源。
4. 推进终端 Agent 部署，实现内网主机安全状态监测。

5.4 漏洞闭环与防护策略

1. 建立漏洞整改台账，优先处置优先修复高危漏洞，分批完成 Apache、Tomcat、SSH、数据库漏洞整改，无法升级的系统做好隔离防护。
2. **建议开启平台旁路阻断编排功能**，实现高风险攻击 IP 自动封堵，降低人工处置压力。
3. 定期开展漏洞扫描、网站安全巡检，做到 “发现- 整改- 复测” 闭环管理。

5.5 安全管理建议

1. 开展师生、运维人员网络安全培训，防范蠕虫病毒、木马，不打开陌生文件链接。
2. 内网做好网络分段隔离，限制中毒主机横向扩散，核心服务器区与办公终端网络隔离。
3. 定期备份网站、业务系统数据，做好应急恢复预案。

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 等服务器高危漏洞、可远程利用漏洞列为第一优先级；对承载官网、报名系统、学生综合管理平台等关键业务的资产漏洞优先处置。明确各业务系统运维负责人，落实 “谁主管、谁运维、谁负责”，避免出现漏洞长期无人处置、整改停滞不前的情况。对于老旧业务系统，无法直接升级补丁的，需要记录系统现状，明确临时防护手段，不允许只登记漏洞而无任何防护措施。

2. 落实漏洞整改- 复测闭环管理，杜绝虚假整改

完善漏洞处置流程，执行 “漏洞发现→下发整改通知→实施修复→漏洞复测→闭环归档” 完整流程。漏洞修复完成之后，不能仅凭运维人员自述完成修复，需要依托咒甲云- 数盾平台重新开展漏洞扫描复测，确认漏洞确实修复完成，方可标记闭环。复测确认未修复的漏洞，需要进行二次督办，

约谈责任运维人员，分析无法修复的根因。对于因业务兼容性问题、系统老旧停产等客观原因，确实不能打补丁修复的漏洞，禁止直接忽略，需要落实补偿防护措施，例如配置防火墙访问策略限制访问源 IP、部署 WAF 规则拦截攻击行为、对受影响资产进行网络隔离，同时做好风险评估，留存风险豁免审批记录，定期复评风险，一旦条件具备立即完成正式修复。针对本次检测发现的 FTP 弱口令`root/root`问题，作为高风险问题立即处置，修改复杂度符合要求的强密码，限制 FTP 服务访问来源，整改完成后开展账号安全专项复测，防止弱口令复现。

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

当前平台已经监测到大量外网攻击行为，累计识别高风险 IP2 个、中风险 IP3 个、低风险 IP133 个，但平台未开启旁路自动阻断编排，所有外部恶意 IP 仅告警记录，无法实现自动封堵，全部依靠人工进行分析处置，防御效率低下，容易错过攻击窗口期。建议尽快完成旁路阻断编排功能上线配置，配置阻断策略：针对暴力破解、漏洞探测、恶意外联、Web 攻击等高风险行为源 IP 实现自动拦截；同时配置阻断白名单，防止校内业务、合作单位合法 IP 被误封；建立阻断日志审计，定期复盘被阻断的攻击 IP，统计攻击趋势。同时明确人工处置流程，对平台告警输出的高危外网攻击源 IP，安排安全运维人员每日巡检研判，对于确认的恶意 IP，执行手动拉黑操作，弥补自动阻断策略覆盖不全的问题。

4. 常态化开展漏洞扫描与安全检测工作

改变“只做月度扫描”的模式，构建常态化扫描机制。主机脆弱性扫描按周期执行，至少每月开展一次；网站脆弱性扫描每两周执行一次；当业务系统上线、版本更新、配置变更之后，要开展临时专项扫描，避免系统变更引入新漏洞。充分利用平台资产测绘能力，及时发现新增互联网暴露资产，做到资产新增即扫描。梳理当前安全运营任务，补齐主机漏洞扫描任务，补齐主机 Agent 部署覆盖率，解决当前主机漏扫任务未执行、Agent 在线数量为 0 的短板。定期对扫描任务执行情况做检查，避免扫描任务失效、扫描任务未正常运行而长期不知情。

5. 漏洞数据汇总分析，驱动系统架构优化

按月度对漏洞数据做统计分析，统计各类漏洞出现频次，梳理高频漏洞类型。针对反复出现的同类漏洞，追溯根源，是开发编码不规范、组件版本管理缺失，还是运维上线流程缺少安全检查。将漏洞统计分析结果同步给开发、运维部门，推动在系统建设、版本上线阶段引入安全检测，从源头减少漏洞产生，把安全要求前置到开发上线环节，而不是仅仅依靠事后扫描修复。

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

针对不同人员群体开展差异化网络安全教育培训。面向全体师生，重点开展终端安全意识培训，讲解蠕虫病毒、木马远控、钓鱼邮件、恶意链接的识别防范方法，引导师生不随意接收、打开陌生邮件附件，不运行来源不明软件，及时更新个人终端系统补丁、杀毒软件病毒库，降低终端被病毒感染概率，从源头减少内网终端非法外联事件。

面向各业务系统运维管理人员，开展专项安全运维培训，培训内容包含互联网暴露面收敛、漏洞修复规范、Web 网站安全防护、恶意事件应急处置、日

志审计等实操内容，提升运维人员安全处置能力。

面向信息化管理部门安全管理人员，重点培训威胁研判、告警分析、安全监测平台使用、网络安全事件应急响应流程，提升整体安全运营能力。

培训形式可结合线下讲座、线上学习、安全案例通报，结合本月月报暴露出的内网大规模中毒、网站黑链、敏感信息泄露等实际风险案例开展警示教育，提升全员风险感知。培训完成后做好培训记录留存。

2. 落实内网网络分区隔离，遏制病毒横向扩散风险

本月监测到 1244 台主机存在非法外联，大量终端感染 xred 蠕虫、银狐木马等恶意程序，内网存在极高横向渗透风险。需要推进内网网络安全分区隔离建设，按照业务属性划分安全域：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，严格限制跨域访问。办公、学生终端域不允许直接访问核心业务服务器，服务器之间最小化开放端口，阻断蠕虫、木马在内网横向传播路径。

对于已经感染病毒的终端，实行隔离处置机制，一旦监测到主机恶意外联、失陷告警，该主机自动隔离至隔离 VLAN，不允许访问内网其他业务，处置完成杀毒验证安全之后才允许恢复网络权限。同时完善网络边界访问控制策略，严格控制内网主机访问互联网恶意站点，对恶意域名、恶意 IP 做 DNS 过滤、访问黑名单。

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、邮箱系统等核心业务系统，落实数据备份策略，采用本地 + 异地备份模式，做好全量备份和增量备份，定期验证备份数据可恢复性，防止发生网站篡改、病毒加密、系统故障后无法恢复业务。

修订完善单位网络安全应急预案，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、数据泄露等典型场景编制处置操作手册。定期组织网络安全应急演练，模拟本次月报中出现的内网大规模蠕虫感染、网站被植入黑链、敏感文件泄露等真实风险场景开展演练，检验运维团队应急处置能力，检验预案可行性，演练结束后复盘，优化应急预案和处置流程。同时明确发生网络安全事件上报机制，一旦发生重大网络安全事件，按照上级主管单位网络安全管理要求及时上报。

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。所有新业务系统上线前，必须完成安全测评，开展漏洞扫描、暴露面核查，禁止存在高危漏洞、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、配置修改之后，要同步开展安全复核检查，避免变更引入新的安全风险。针对新增互联网 Web 资产，第一时间纳入安全监测范围，及时发现新增暴露风险。

完善第三方外包开发运维管理，对外包建设网站、业务系统，明确网络安全责任，要求外包单位遵循安全开发规范，交付系统必须完成安全自查，定期对外包维护的网站开展安全抽查，防范因外包人员运维不当带来黑链、漏洞、信息泄露风险。

5. 健全常态化巡检考核机制，推动安全风险闭环落地

建立月度网络安全风险巡检制度，依托咒甲云-数盾平台输出月报，跟踪上月风险整改完成情况，对逾期未整改的风险进行持续督办。将网络安全

风险整改落实情况纳入运维岗位工作考核，提高运维人员对网络安全工作重视程度。

定期开展资产梳理，持续摸清互联网 **Web** 资产、内网服务器、终端资产台账，杜绝出现资产 “看不见、管不到” 的情况。定期复盘安全监测平台告警质量，优化告警规则，减少无效告警，提升安全人员研判效率。

建立风险定期通报机制，按月向各业务部门通报本部门业务系统存在的安全风险，压实业务部门主体责任，形成 “监测- 通报- 整改- 复测- 考核” 的常态化安全管理闭环。

6. 推进安全能力补齐建设

当前存在主机 **Agent** 部署覆盖率为 0，终端监测能力缺失问题，分步推进终端安全 **Agent** 部署工作，逐步实现内网服务器、重要终端的 **Agent** 全覆盖，实现主机日志采集、异常行为监测、病毒查杀、基线核查能力，改变仅依靠外部扫描的被动防御现状。

结合风险现状评估 **WAF**、堡垒机等安全设备使用效果，对于直接暴露公网的业务系统完善 **WAF** 防护规则，对于后台管理访问场景推广堡垒机运维，减少直接对公网开放管理端口、管理后台的情况。