东北财经大学
DONGBEI UNIVERSITY OF FINANCE & ECONOMICS

网络安全态势月报

智慧校园建设中心

2026年05月

目录 CONTENTS

01 内部网络安全情况 - 网络安全整体解读

网络安全整体解读-安全总览

- 共捕获攻击次数1.87千万次,较上个月增加58.16%；平均每日捕获攻击近60.33万次，攻击者数量达1.52万个，来源国家或地区157个，境外主要来自美国、新加坡、英国，境内主要是河北、辽宁、北京。外部攻击形势依旧严峻；
- 共捕获恶意程序事件125次；网络攻击事件50次；未发生网络探测事件、网络异常事件；
- 共捕获漏洞0个；弱密码15个；

1.87千万次	1.52万个	122个	125个	50个	41个	0个	15个
攻击总数	攻击者	境外攻击地区	恶意程序事件	网络攻击事件	其他	漏洞总数	弱密码账号

境外攻击源地区

境内攻击源地区

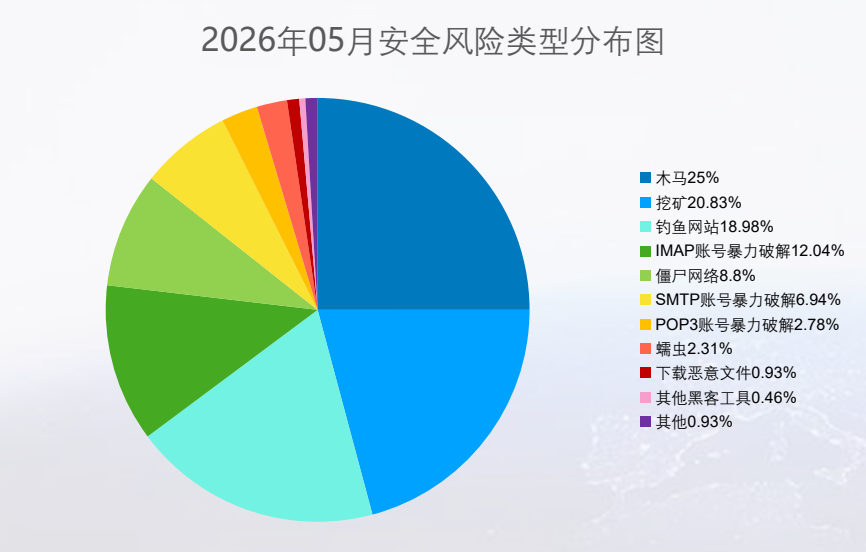
安全风险类型分布

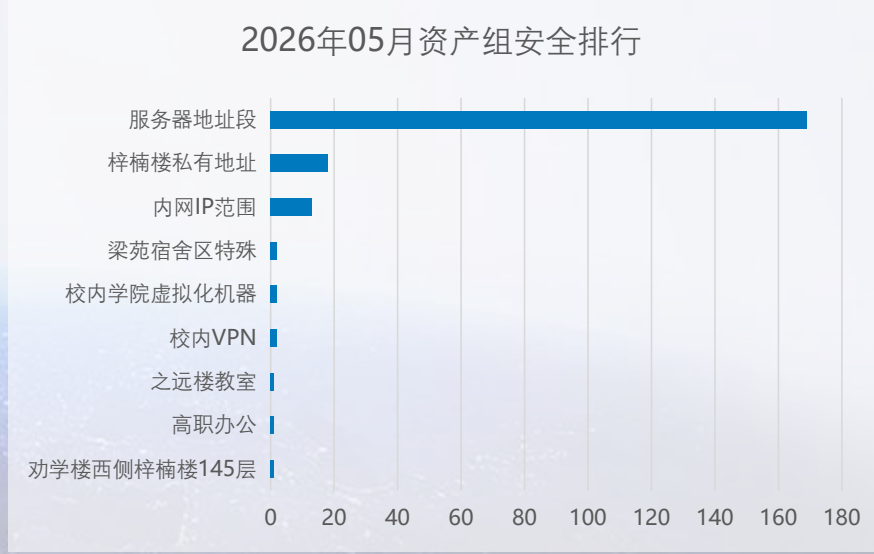
漏洞分布图

暂无数据

网络安全整体解读-安全总览

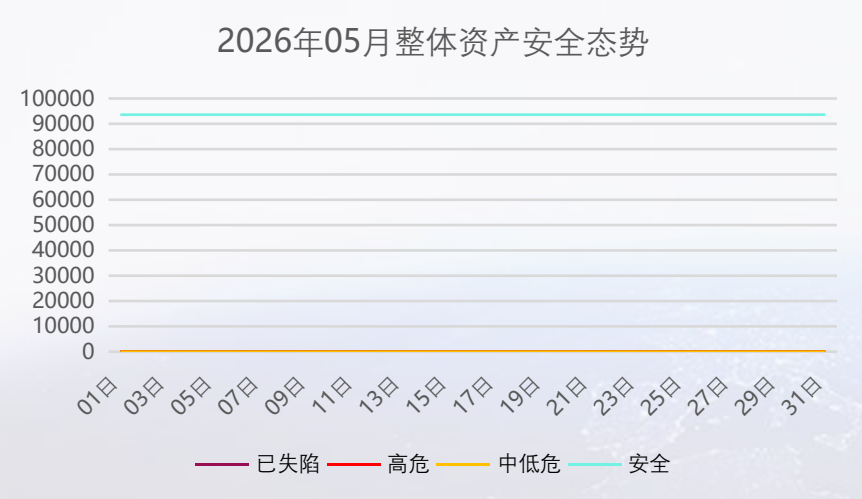
- 2026年05月最突出的安全风险前三名分别是木马、挖矿、钓鱼网站，本月处理这三类风险分别为25%、20.83%、18.98%，占本月总风险64.81%；针对这些风险，共处置主机36个/次，处置漏洞0个；
- 按资产组分布，发生安全风险次数最多的是服务器地址段，共169次，占总数的78.24%；其次是梓楠楼私有地址（18次，8.33%）、内网IP范围（13次，6.02%）；安全风险次数最少的是之远楼教室、高职办公、劝学楼西侧梓楠楼145层。





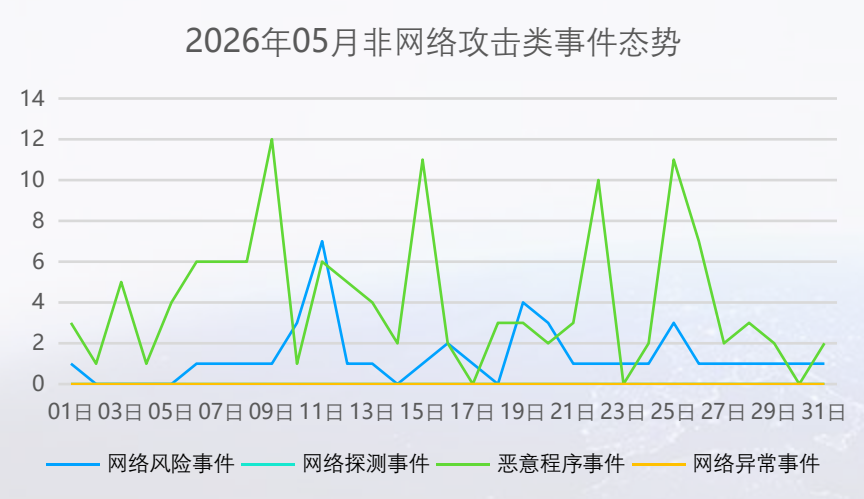
网络安全整体解读-安全态势

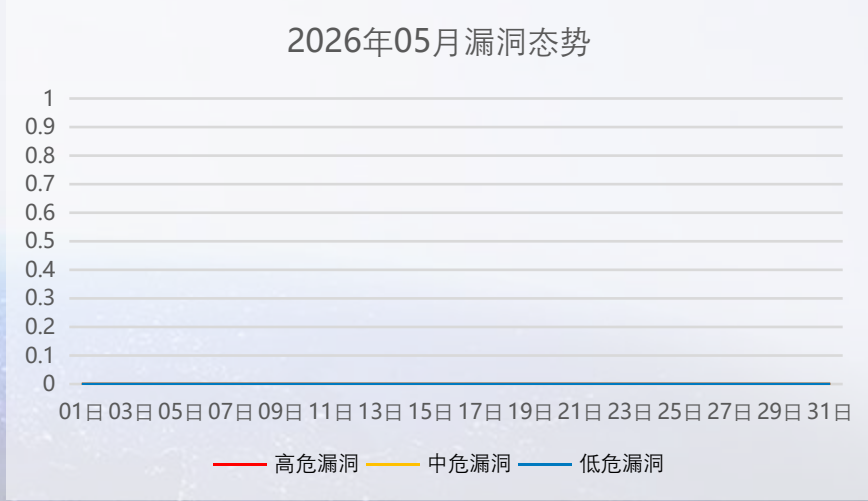
- 2026年05月平均每日捕获风险资产4.45个左右，占总资产数（服务器210个、终端92762个）0%；风险资产总数在5月11日达到高峰，共10个，占资产总数0.01%；“已失陷”资产在5月24日增幅最大，增幅达400%，从1个增加到5个；“已失陷”资产数在5月23日经过处置后，同比减少83.33%；“高危”资产在5月11日增幅最大，增幅达200%，从1个增加到3个；“高危”资产数在5月2日经过处置后，同比减少100%；“安全”类资产在5月3日至5月5日、5月11日至5月13日等出现连续3日以上的持续增长；“安全”类资产在5月1日至5月3日、5月7日至5月9日等出现连续3日以上的持续减少；
- 2026年05月共捕获外部网络攻击1.87千万次，平均每日60.33万次；较上个月增加58.16%；在5月21日达到最高的74.16万次；波动最大的是5月15日，较5月14日增加29.17%；在5月1日至5月3日、5月4日至5月6日等出现连续3日以上的持续增长。在5月6日至5月8日、5月9日至5月12日等出现连续3日以上的持续减少。



网络安全整体解读-安全态势

- 2026年05月共捕获有害程序、信息破坏、信息内容安全等其他非网络攻击类事件216次，日均6.97次，其中5月25日最高14次；
- 2026年05月共捕获漏洞0个，平均每日0个；捕获次数最高的是5月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；
- 其中高危漏洞0个，占比100%，平均每日0个；高危漏洞捕获次数最高的是5月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；

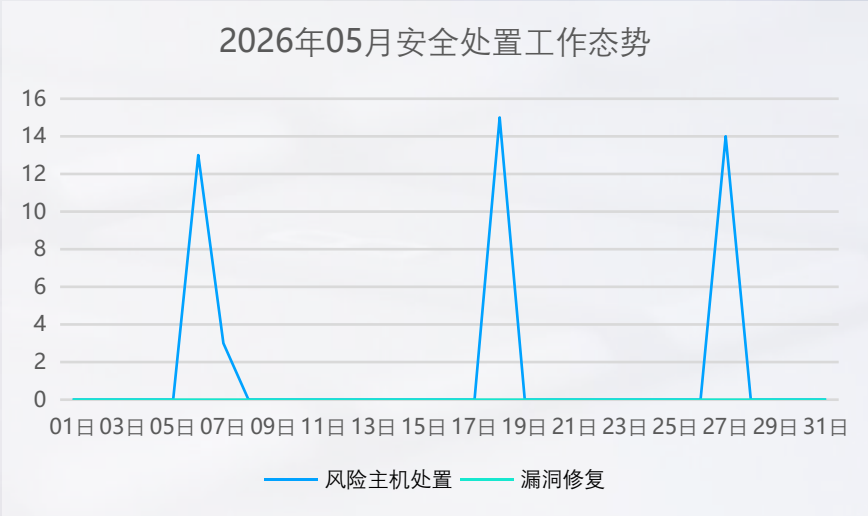




网络安全整体解读-安全处置工作概览

- 2026年05月共处置风险主机45个，较上个月减少21.05%；修复漏洞0个， 另有合规检查0次、重大活动保障0次，有效保障了我方网络安全。

攻击捕获	1.87千万次
修复漏洞	0次
处置主机	45条
合规检查	0次
重大活动保障	0次



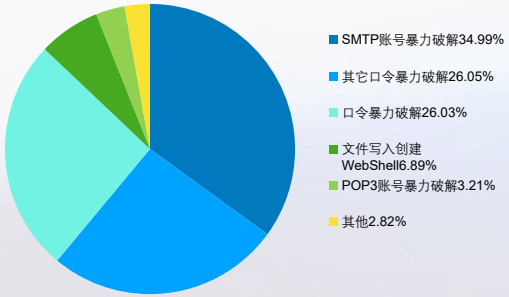
01 内部网络安全情况 - 网络安全风险详情

—— 本章节将详细阐述暴力破解、网站攻击、邮件安全、僵尸网络、恶意程序、业务脆弱性的捕获统计和趋势分析

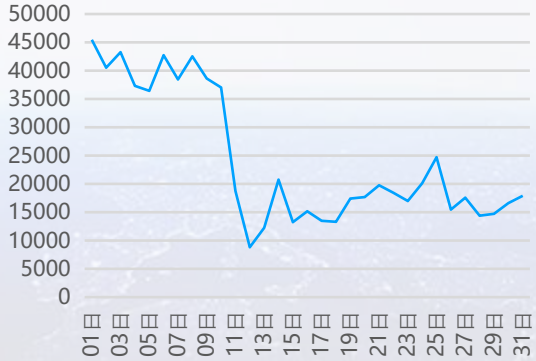
网络安全风险详情-横向威胁

- 在2026年05月共捕获横向威胁主机603台，横向威胁事件74.98万件，其中SMTP账号暴力破解排名第一，占比34.99%；其次是其它口令暴力破解、口令暴力破解。
- 趋势上，平均每日发起横向威胁2.42万件；捕获次数最多的是5月1日，达4.55万次；波动最大的是5月12日，较5月11日减少52.93%；在5月12日至5月14日、5月18日至5月21日等出现连续3日以上的持续增长。在5月3日至5月5日、5月8日至5月12日等出现连续3日以上的持续减少。
- 按资产组分布，发生横向威胁最多的是校内学院虚拟化机器，共63.13万次，占总数的84.2%；其次是锐捷交换机（6.42万次，8.56%）、内网IP范围（4.81万次，6.41%）等。

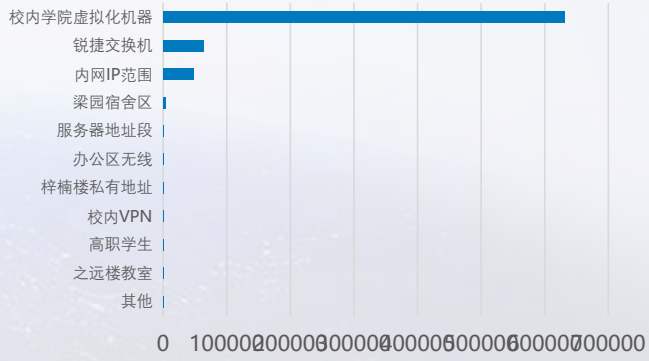
横向威胁类型分布



横向威胁趋势图

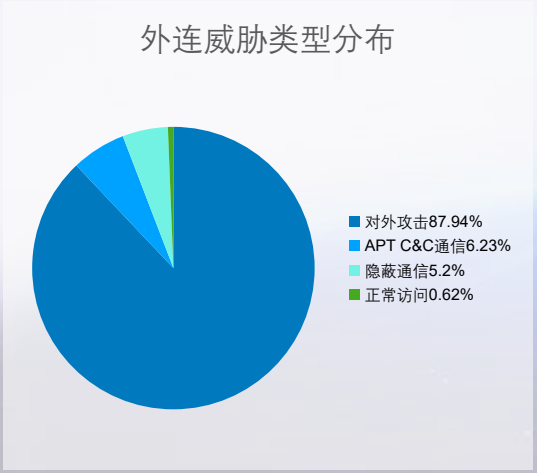


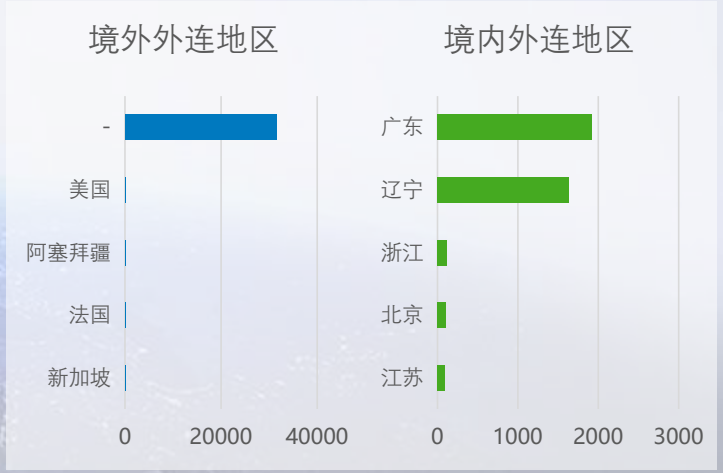
遭受横向威胁分支排行



网络安全风险详情-外连威胁

- 在2026年05月共捕获外连威胁主机145台，外连威胁事件3.6万件，其中对外攻击排名第一，占比87.94%；其次是APT C&C通信、隐蔽通信。
- 趋势上，平均每日发起外连威胁1161.06件；捕获次数最多的是5月15日，达2055次；波动最大的是5月16日，较5月15日减少49.15%；在5月23日至5月26日、5月27日至5月29日出现连续3日以上的持续增长。在5月8日至5月10日、5月15日至5月17日出现连续3日以上的持续减少。
- 风险主机外连地区既有境内也有境外；境外外连地区主要来自-、美国、阿塞拜疆、法国、新加坡，这5个国家/地区的外连次数占总体境外外连地区的99.91%；境内主要来源广东、辽宁、浙江、北京、江苏，这5个省份的外连次数占总体外连次数90.23%，占总外连次数的10.75%；

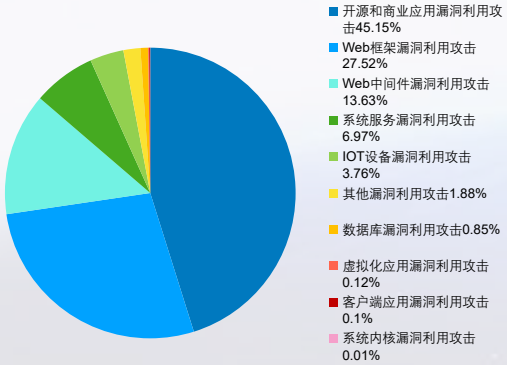




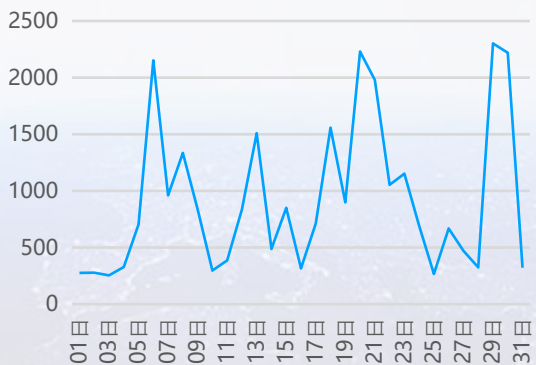
网络安全风险详情-漏洞利用

- 漏洞利用是最常见的一种网络攻击，2026年05月共捕获漏洞利用攻击告警2.87万次，其中开源和商业应用漏洞利用攻击排名第一，占比45.15%；其次是Web框架漏洞利用攻击、Web中间件漏洞利用攻击。
- 趋势上，平均每日发起漏洞利用攻击924.52件；捕获次数最多的是5月29日，达2302次；波动最大的是5月29日，较5月28日增加608.31%；在5月3日至5月6日、5月10日至5月13日等出现连续3日以上的持续增长。在5月8日至5月10日、5月20日至5月22日等出现连续3日以上的持续减少。
- 按资产组分布，发生漏洞利用攻击最多的是服务器地址段，共1.05万次，占总数的42.7%；其次是校内学院虚拟化机器（9729次，39.43%）、内网IP范围（3243次，13.14%）等。

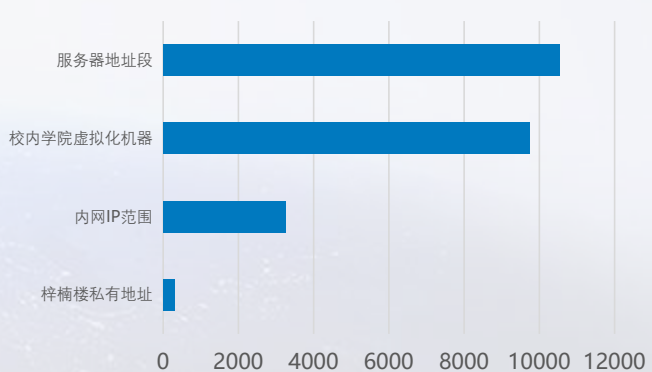
漏洞利用攻击类型



漏洞利用趋势图

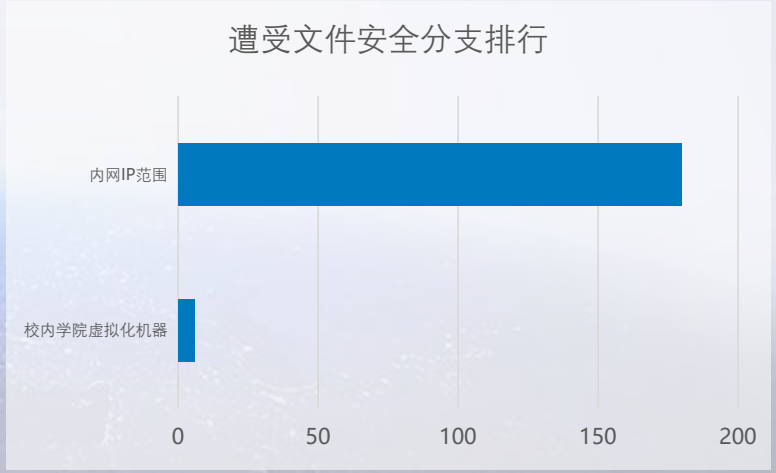


遭受漏洞利用攻击分支排行



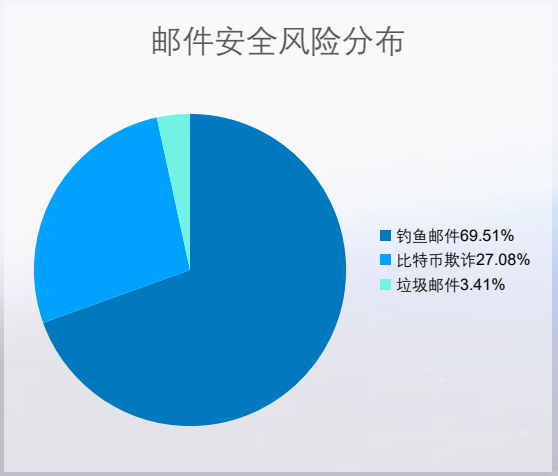
网络安全风险详情-文件安全

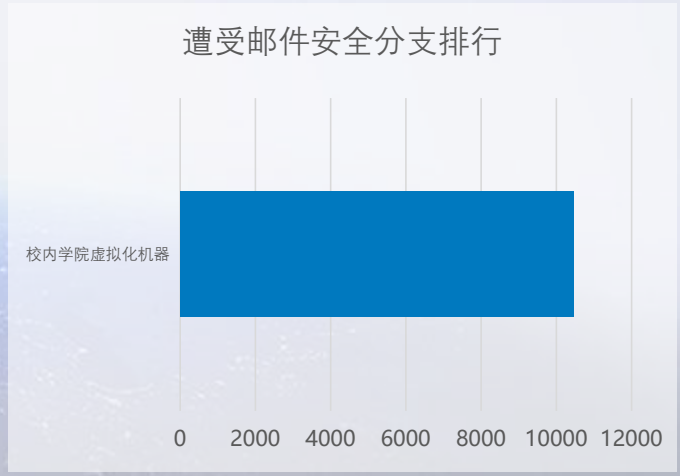
- 文件是病毒传播的常见手段；2026年05月共查杀文件770074余次，确认为恶意文件的有186个；
- 趋势上，平均每日捕获恶意文件6件；审计次数最多的是5月9日，达19次；波动最大的是5月22日，较5月21日增加1700%；在5月20日至5月22日出现连续3日以上的持续增长。
- 按资产组分布，发生文件安全最多的是内网IP范围，共180次，占总数的96.77%；其次是校内学院虚拟化机器（6次，3.23%）等。



网络安全风险详情-邮件安全

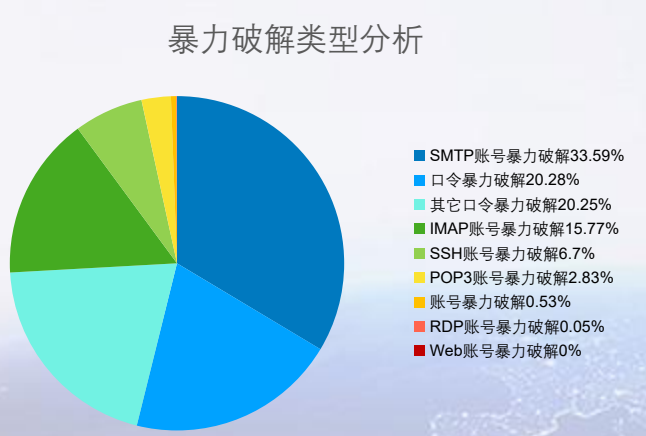
- 邮件是恶意软件分发和网络钓鱼的头号媒介；2026年05月，共捕获钓鱼邮件69.51%7267次；比特币欺诈27.08%2831次；垃圾邮件3.41%357次；
- 趋势上，平均每日捕获邮件安全风险337.26件；捕捉最高的是5月7日，达1157次；波动最大的是5月6日，较5月5日增加736.36%；在5月3日至5月7日、5月10日至5月12日等出现连续3日以上的持续增长。在5月1日至5月3日、5月7日至5月10日等出现连续3日以上的持续减少。
- 按资产组分布，发生邮件安全最多的是校内学院虚拟化机器，共1.05万次，占总数的100%；





网络安全风险详情-暴力破解

- 暴力破解是最常见的一种网络攻击，2026年05月共捕获暴力破解攻击告警22.8万次，其中SMTP账号暴力破解排名第一，占比33.59%;其次是口令暴力破解、其它口令暴力破解。
- 暴破频率最高达901次/分钟，该告警于2026年05月19日22时16分捕获，来自于-攻击者118.202.165.10攻击校内学院虚拟化机器的服务器202.199.162.124



捕获时间：	2026-05-19 22:16:16
攻击者：	118.202.165.10（-）
攻击手段：	账号暴力破解
暴破频率：	最高达901次/分钟
受害者：	校内学院虚拟化机器（202.199.162.124）

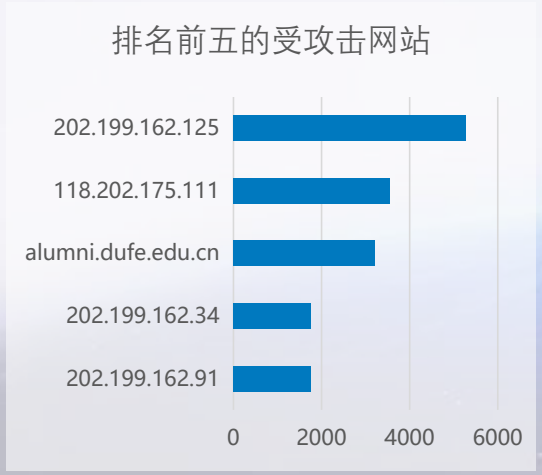
网络安全风险详情-业务脆弱性

- 业务脆弱性是指“资产中能被威胁所利用的弱点”，包括技术层面的脆弱性，如：漏洞、WEB明文传输、配置错误，还有管理层面的风险，如：弱密码。2026年05月共捕获漏洞0个，Web明文传输185个，配置错误风险237个，弱密码账号82个；
- 捕获最多的是-，共捕获0次，占所有漏洞的0%；
- 平均每日捕获高危漏洞0个；捕获次数最多的是5月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；

0个	185个	237个	82个
漏洞	Web明文传输	配置风险	弱密码

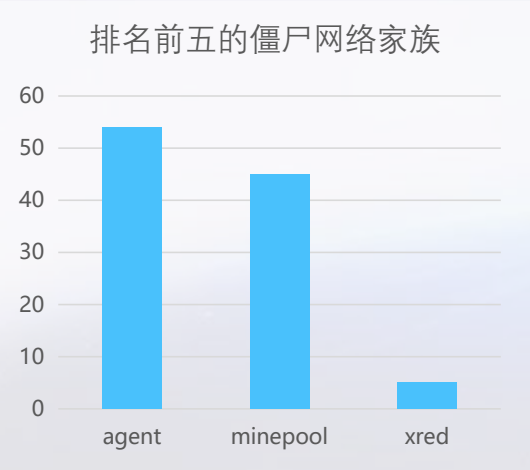
网络安全风险详情-网站攻击

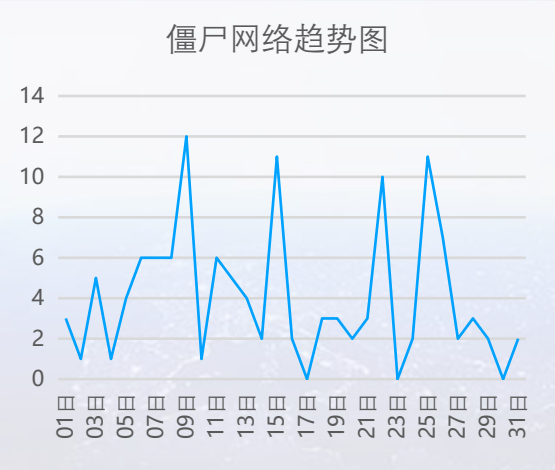
- 2026年05月，共捕获网站类攻击5.09万次，其中被攻击最多的网站是202.199.162.125，达到5279次，占总体的10.36%；其次是118.202.175.111、alumni.dufe.edu.cn。
- 2026年05月捕获的网站攻击中，既有来自境内的，也有来自境外的；境外攻击源主要来自美国、加拿大、德国、英国、巴西，这5个国家/地区的网站攻击占总体境外网站攻击的57.43%；境内主要来源辽宁、吉林、广东、香港、北京，这5个省份的网站攻击占总体境内网站攻击80.29%，占所有网站攻击的41.68%；
- 趋势上，平均每日捕获网络攻击1643.06次；捕获次数最高的是5月20日，达6036次；波动最大的是5月6日，较5月5日增加1223.23%；在5月1日至5月3日、5月11日至5月13日出现连续3日以上的持续增长。在5月3日至5月5日、5月15日至5月17日等出现连续3日以上的持续减少。

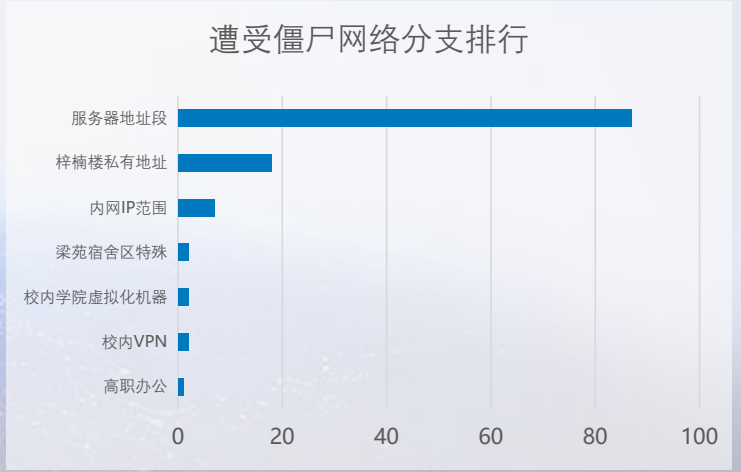


网络安全风险详情-僵尸网络

- 2026年05月，共捕获僵尸网络125次；其中agent家族是攻击态势最为活跃的僵尸网络家族，占所有僵尸网络拦截数量的43.2%；排名第二第三的minepool、xred比例分别为36%、4%
- 趋势上，平均每日捕获僵尸网络攻击4.03次；捕获次数最高的是5月9日，达12次；波动最大的是5月11日，较5月10日增加500%；在5月4日至5月6日、5月20日至5月22日等出现连续3日以上的持续增长。在5月11日至5月14日、5月15日至5月17日等出现连续3日以上的持续减少。
- 按资产组分布，发生僵尸网络最多的是服务器地址段，共87次，占总数的69.6%；其次是梓楠楼私有地址（18次，14.4%）、内网IP范围（7次，5.6%）等。

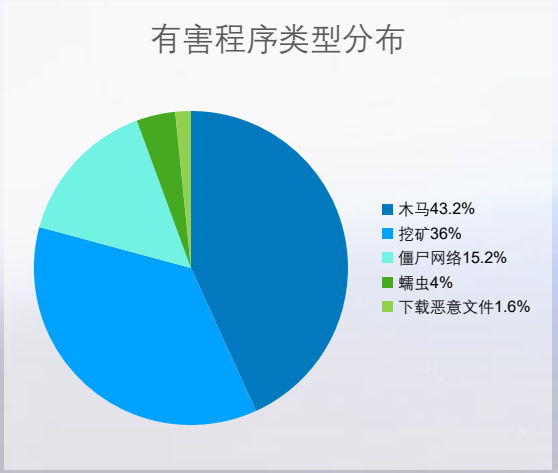


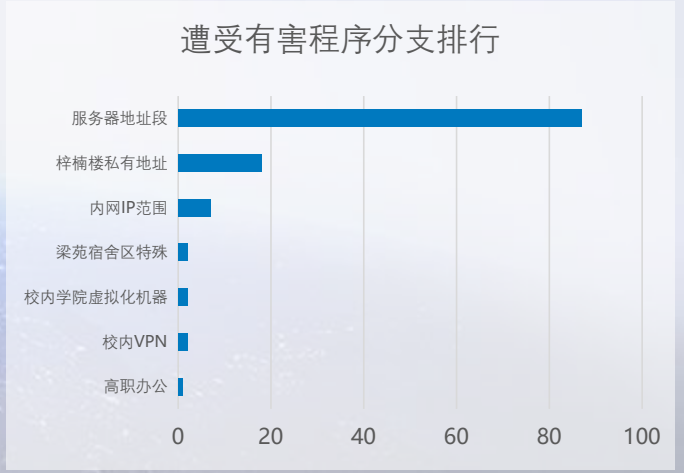




网络安全风险详情-有害程序

- 2026年05月，共捕获有害程序告警125次；其中最为活跃的是木马，共捕获54次，占所有恶意程序捕获数量的43.2%；而排名第二第三的挖矿、僵尸网络的比例分别为36%、15.2%
- 趋势上，平均每日捕获有害程序风险4.03次；捕获次数最高的是5月9日，达12次；波动最大的是5月11日，较5月10日增加500%；在5月4日至5月6日、5月20日至5月22日等出现连续3日以上的持续增长。在5月11日至5月14日、5月15日至5月17日等出现连续3日以上的持续减少。
- 按资产组分布，发生有害程序最多的是服务器地址段，共87次，占总数的69.6%；其次是梓楠楼私有地址（18次，14.4%）、内网IP范围（7次，5.6%）等。





THANK YOU

2026年05月