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

2025年06月

目录 CONTENTS

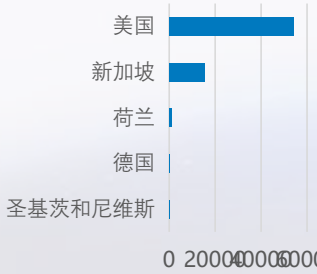
01 内部网络安全情况 - 网络安全整体解读

网络安全整体解读-安全总览

- 共捕获攻击次数1.36百万次,较上个月减少28.18%；平均每日捕获攻击近4.53万次，攻击者数量达3.37万个，来源国家或地区112个，境外主要来自美国、新加坡、荷兰，境内主要是河北、北京、湖北。外部攻击形势依旧严峻；
- 共捕获恶意程序事件182次；网络攻击事件136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；

1.36百万次	3.37万个	77个	182个	136个	18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

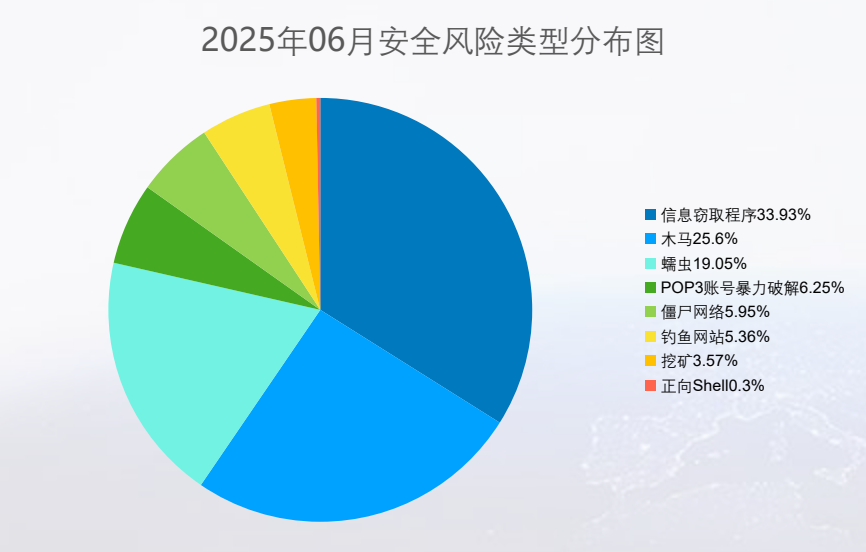
安全风险类型分布

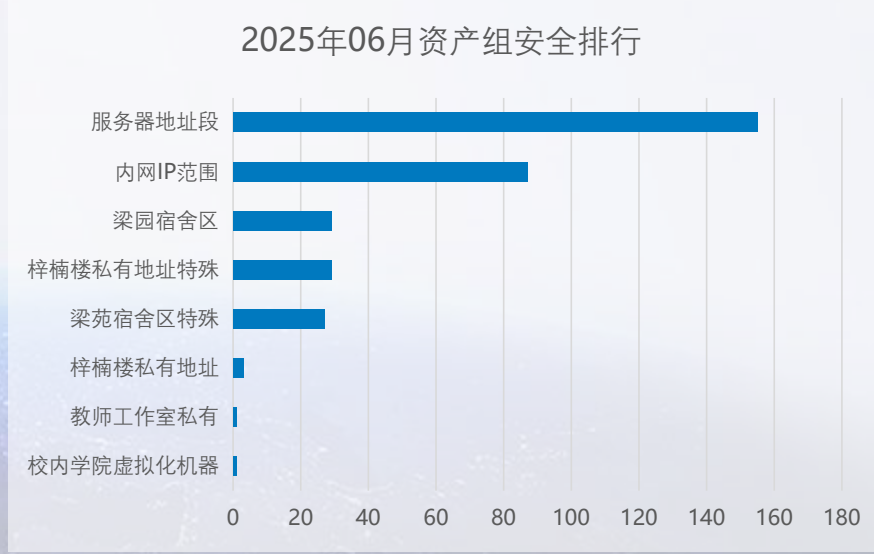
漏洞分布图

暂无数据

网络安全整体解读-安全总览

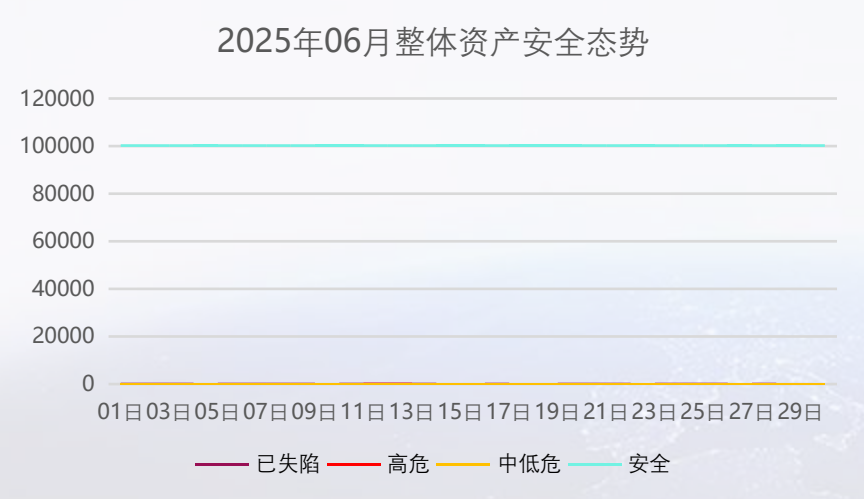
- 2025年06月最突出的安全风险前三名分别是信息窃取程序、木马、蠕虫，本月处理这三类风险分别为33.93%、25.6%、19.05%，占本月总风险78.57%；针对这些风险，共处置主机101个/次，处置漏洞0个；
- 按资产组分布，发生安全风险次数最多的是服务器地址段，共155次，占总数的46.13%；其次是内网IP范围（87次，25.89%）、梁园宿舍区（29次，8.63%）；安全风险次数最少的是梓楠楼私有地址、教师工作室私有、校内学院虚拟化机器。





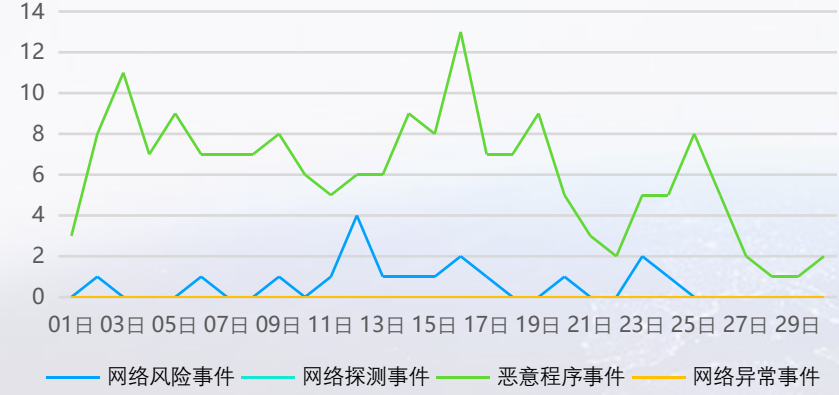
网络安全整体解读-安全态势

- 2025年06月平均每日捕获风险资产8.23个左右，占总资产数（服务器222个、终端99365个）0.01%；风险资产总数在6月3日达到高峰，共12个，占资产总数0.01%；“已失陷”资产在6月7日增幅最大，增幅达37.5%，从8个增加到11个；“已失陷”资产数在6月26日经过处置后，同比减少25%；“高危”资产数在6月13日经过处置后，同比减少100%；“安全”类资产在6月7日至6月9日、6月19日至6月22日出现连续3日以上的持续增长；“安全”类资产在6月1日至6月3日、6月23日至6月25日出现连续3日以上的持续减少；
- 2025年06月共捕获外部网络攻击1.36百万次，平均每日4.53万次；较上个月减少28.18%；在6月26日达到最高的8.3万次；波动最大的是6月9日，较6月8日减少62.02%；在6月5日至6月8日、6月9日至6月12日等出现连续3日以上的持续增长。在6月1日至6月5日、6月14日至6月16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

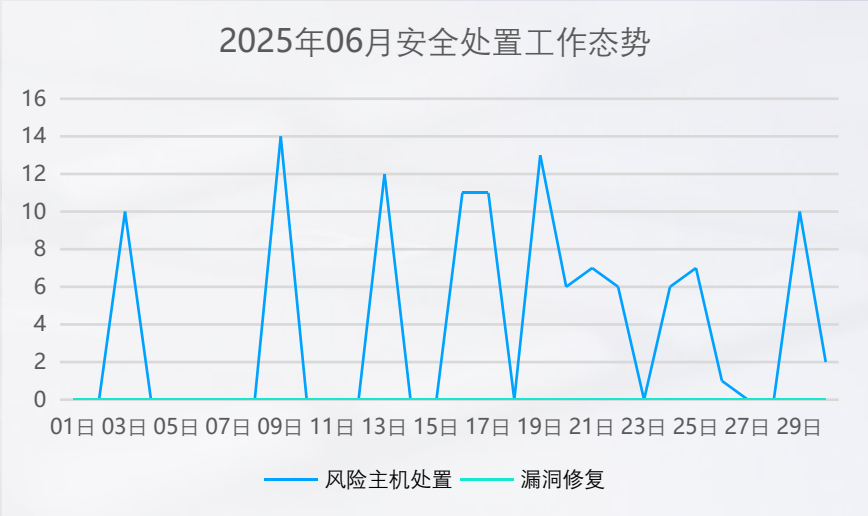
- 2025年06月共捕获有害程序、信息破坏、信息内容安全等其他非网络攻击类事件336次，日均11.2次，其中6月16日最高15次；
- 2025年06月共捕获漏洞0个，平均每日0个；捕获次数最高的是6月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；
- 其中高危漏洞0个，占比100%，平均每日0个；高危漏洞捕获次数最高的是6月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；



网络安全整体解读-安全处置工作概览

- 2025年06月共处置风险主机116个，较上个月减少82.26%；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	1.36百万次
修复漏洞	0次
处置主机	116条
合规检查	0次
重大活动保障	0次

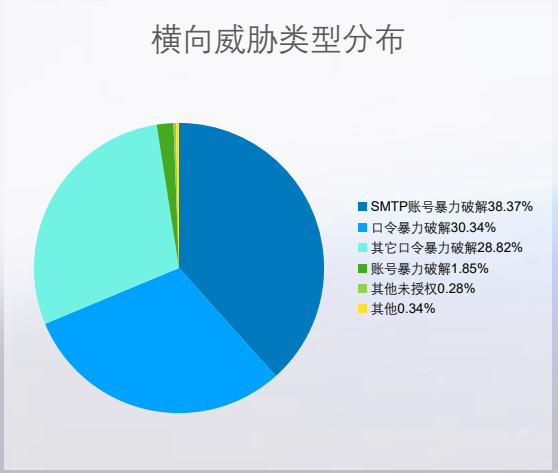


01 内部网络安全情况 - 网络安全风险详情

—— 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

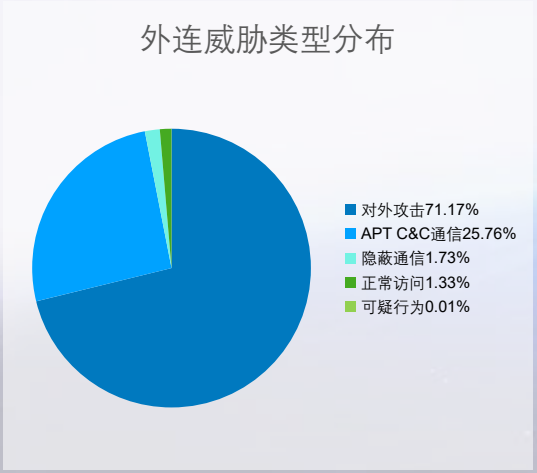
网络安全风险详情-横向威胁

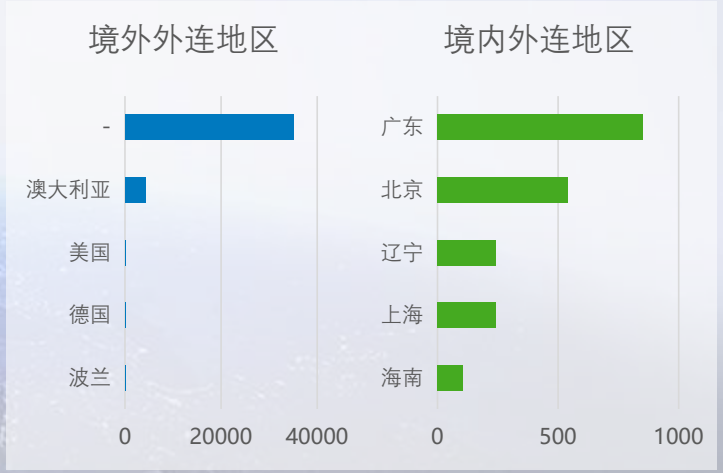
- 在2025年06月共捕获横向威胁主机562台，横向威胁事件4.02百万件，其中SMTP账号暴力破解排名第一，占比38.37%；其次是口令暴力破解、其它口令暴力破解。
- 趋势上，平均每日发起横向威胁13.41万件；捕获次数最多的是6月17日，达28.55万次；波动最大的是6月29日，较6月28日减少61.16%；在6月1日至6月3日、6月7日至6月10日等出现连续3日以上的持续增长。在6月5日至6月7日、6月19日至6月23日等出现连续3日以上的持续减少。
- 按资产组分布，发生横向威胁最多的是校内学院虚拟化机器，共3.64百万次，占总数的90.51%；其次是锐捷交换机（25.14万次，6.25%）、内网IP范围（10.3万次，2.56%）等。



网络安全风险详情-外连威胁

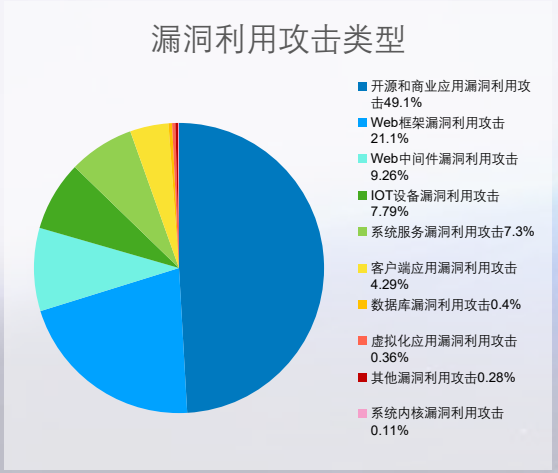
- 在2025年06月共捕获外连威胁主机334台，外连威胁事件4.23万件，其中对外攻击排名第一，占比71.17%；其次是APT C&C通信、隐蔽通信。
- 趋势上，平均每日发起外连威胁1409.6件；捕获次数最多的是6月13日，达1737次；波动最大的是6月18日，较6月17日减少25.87%；在6月8日至6月11日、6月21日至6月23日出现连续3日以上的持续增长。在6月2日至6月6日、6月13日至6月15日等出现连续3日以上的持续减少。
- 风险主机外连地区既有境内也有境外；境外外连地区主要来自-、澳大利亚、美国、德国、波兰，这5个国家/地区的外连次数占总体境外外连地区的99.89%；境内主要来源广东、北京、辽宁、上海、海南，这5个省份的外连次数占总体外连次数74.13%，占总外连次数的4.68%；





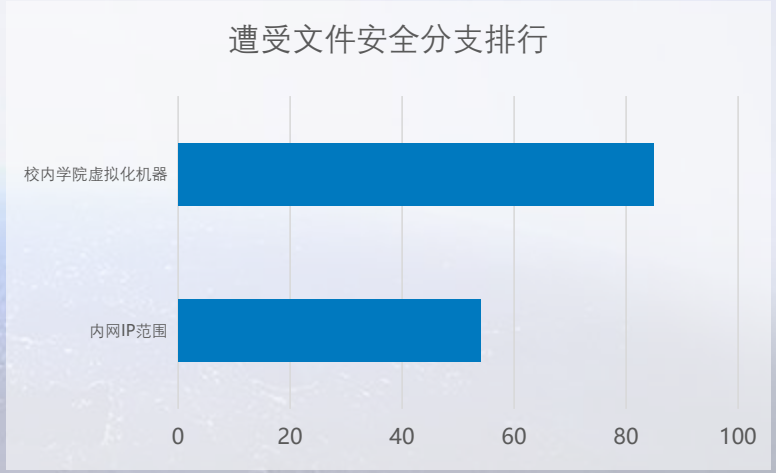
网络安全风险详情-漏洞利用

- 漏洞利用是最常见的一种网络攻击，2025年06月共捕获漏洞利用攻击告警2.55万次，其中开源和商业应用漏洞利用攻击排名第一，占比49.1%；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850.2件；捕获次数最多的是6月25日，达8237次；波动最大的是6月13日，较6月12日减少97.75%；在6月14日至6月18日、6月22日至6月25日等出现连续3日以上的持续增长。在6月12日至6月14日、6月18日至6月20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1.55万次，占总数的71.43%；其次是校内学院虚拟化机器（4300次，19.87%）、内网IP范围（1484次，6.86%）等。



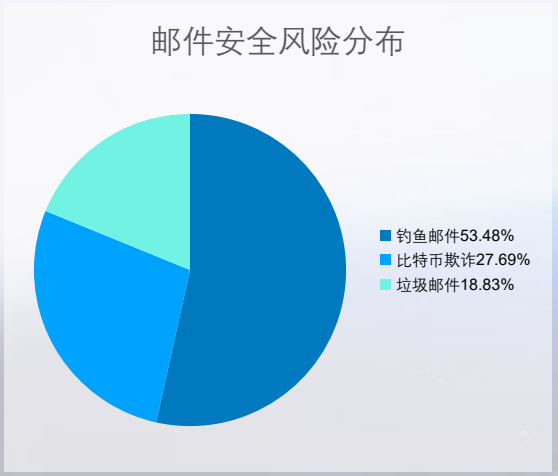
网络安全风险详情-文件安全

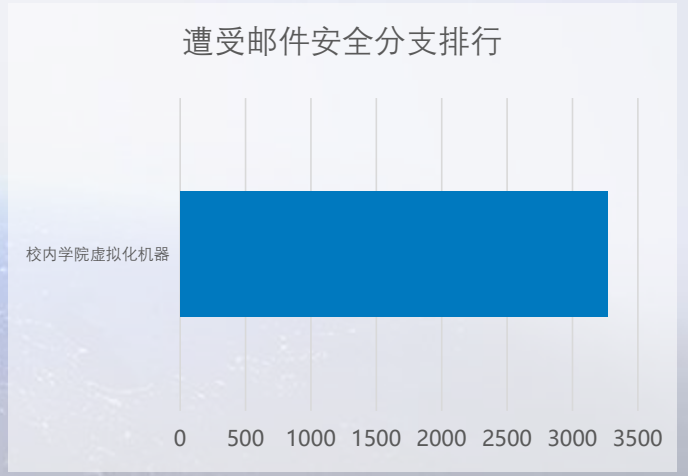
- 文件是病毒传播的常见手段；2025年06月共查杀文件1124042余次，确认为恶意文件的有150个；
- 趋势上，平均每日捕获恶意文件5件；审计次数最多的是6月20日，达33次；波动最大的是6月2日，较6月1日减少100%；在6月11日至6月13日、6月15日至6月17日等出现连续3日以上的持续增长。在6月20日至6月22日、6月25日至6月28日出现连续3日以上的持续减少。
- 按资产组分布，发生文件安全最多的是校内学院虚拟化机器，共85次，占总数的56.67%；其次是内网IP范围（54次，36%）等。



网络安全风险详情-邮件安全

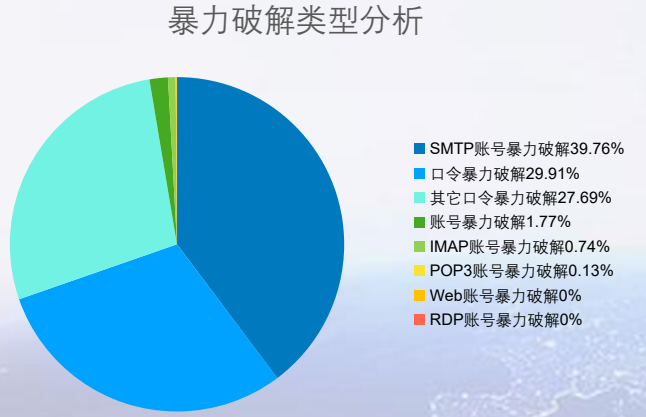
- 邮件是恶意软件分发和网络钓鱼的头号媒介；2025年06月，共捕获钓鱼邮件53.48%1750次；比特币欺诈27.69%906次；垃圾邮件18.83%616次；
- 趋势上，平均每日捕获邮件安全风险109.07件；捕捉最高的是6月8日，达980次；波动最大的是6月8日，较6月7日增加8809.09%；在6月11日至6月13日、6月14日至6月16日等出现连续3日以上的持续增长。在6月1日至6月7日、6月20日至6月22日等出现连续3日以上的持续减少。
- 按资产组分布，发生邮件安全最多的是校内学院虚拟化机器，共3272次，占总数的100%；





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，2025年06月共捕获暴力破解攻击告警2.73百万次，其中SMTP账号暴力破解排名第一，占比39.76%;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2025年06月05日07时03分捕获，来自于-攻击者118.202.165.12攻击校内学院虚拟化机器的服务器202.199.162.125



捕获时间：	2025-06-05 07:03:40
攻击者：	118.202.165.12（-）
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（202.199.162.125）

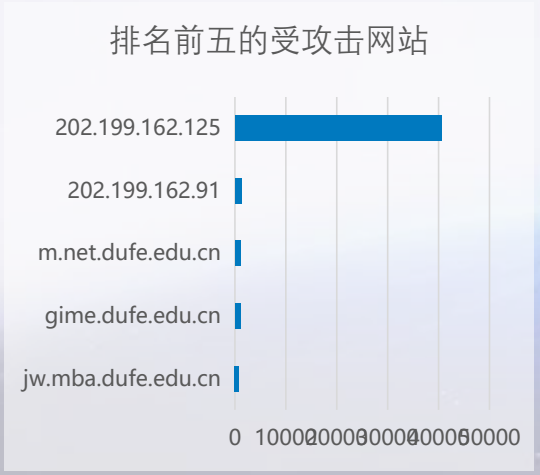
网络安全风险详情-业务脆弱性

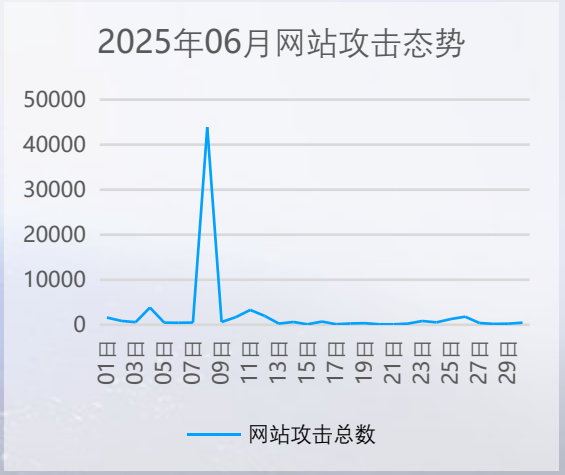
- 业务脆弱性是指“资产中能被威胁所利用的弱点”，包括技术层面的脆弱性，如：漏洞、WEB明文传输、配置错误，还有管理层面的风险，如：弱密码。2025年06月共捕获漏洞0个，Web明文传输190个，配置错误风险119个，弱密码账号38个；
- 捕获最多的是-，共捕获0次，占所有漏洞的0%；
- 平均每日捕获高危漏洞0个；捕获次数最多的是6月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；

0个	190个	119个	38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

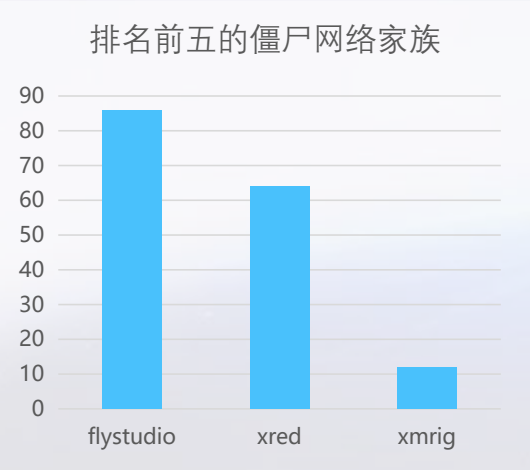
- 2025年06月，共捕获网站类攻击6.85万次，其中被攻击最多的网站是202.199.162.125，达到4.05万次，占总体的59.16%；其次是202.199.162.91、m.net.dufe.edu.cn。
- 2025年06月捕获的网站攻击中，既有来自境内的，也有来自境外的；境外攻击源主要来自美国、荷兰、圣基茨和尼维斯、德国、新加坡，这5个国家/地区的网站攻击占总体境外网站攻击的97.18%；境内主要来源浙江、黑龙江、山东、辽宁、湖北，这5个省份的网站攻击占总体境内网站攻击88.21%，占所有网站攻击的27.11%；
- 趋势上，平均每日捕获网络攻击2283次；捕获次数最高的是6月8日，达4.39万次；波动最大的是6月8日，较6月7日增加8820.33%；在6月6日至6月8日、6月9日至6月11日等出现连续3日以上的持续增长。在6月1日至6月3日、6月4日至6月6日等出现连续3日以上的持续减少。

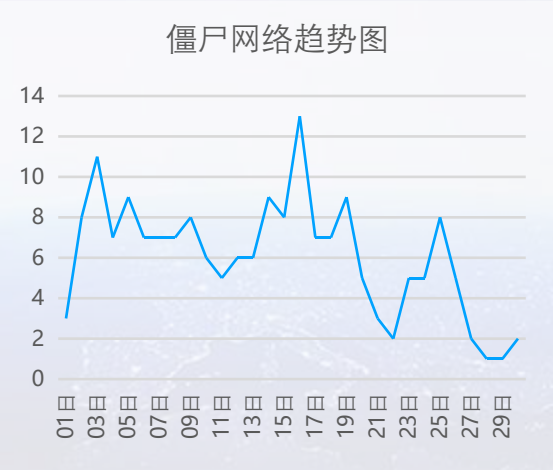


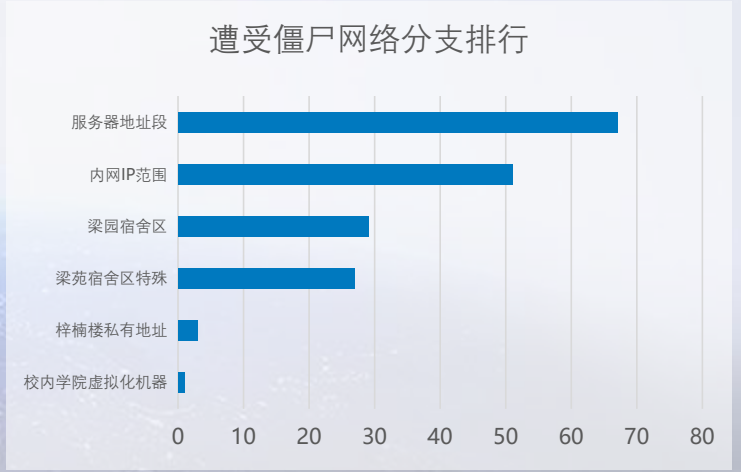


网络安全风险详情-僵尸网络

- 2025年06月，共捕获僵尸网络182次；其中flystudio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47.25%；排名第二第三的xred、xmrig比例分别为35.16%、6.59%
- 趋势上，平均每日捕获僵尸网络攻击6.07次；捕获次数最高的是6月16日，达13次；波动最大的是6月2日，较6月1日增加166.67%；在6月1日至6月3日出现连续3日以上的持续增长。在6月9日至6月11日、6月19日至6月22日等出现连续3日以上的持续减少。
- 按资产组分布，发生僵尸网络最多的是服务器地址段，共67次，占总数的36.81%；其次是内网IP范围（51次，28.02%）、梁园宿舍区（29次，15.93%）等。

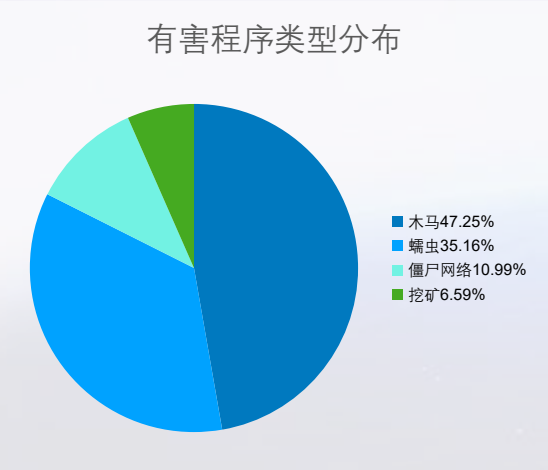


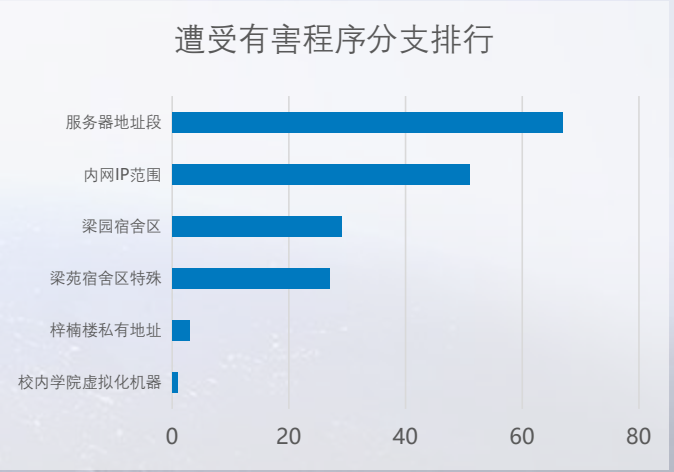




网络安全风险详情-有害程序

- 2025年06月，共捕获有害程序告警182次；其中最为活跃的是木马，共捕获86次，占所有恶意程序捕获数量的47.25%；而排名第二第三的蠕虫、僵尸网络的比例分别为35.16%、10.99%
- 趋势上，平均每日捕获有害程序风险6.07次；捕获次数最高的是6月16日，达13次；波动最大的是6月2日，较6月1日增加166.67%；在6月1日至6月3日出现连续3日以上的持续增长。在6月9日至6月11日、6月19日至6月22日等出现连续3日以上的持续减少。
- 按资产组分布，发生有害程序最多的是服务器地址段，共67次，占总数的36.81%；其次是内网IP范围（51次，28.02%）、梁园宿舍区（29次，15.93%）等。





THANK YOU

2025年06月