网络安全态势月报

智慧校园建设中心

2026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2.12千万次,较上个月增加13.23%；平均每日捕获攻击近70.59万次，攻击者数量达5.16万个，来源国家或地区165个，境外主要来自美国、法国、新加坡，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147次；网络攻击事件48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38个；

2.12千万次	5.16万个	130个
攻击总数	攻击者	境外攻击地区

147个	48个	36个
恶意程序事件	网络攻击事件	其他

0个	38个
漏洞总数	弱密码账号

境外攻击源地区

境内攻击源地区

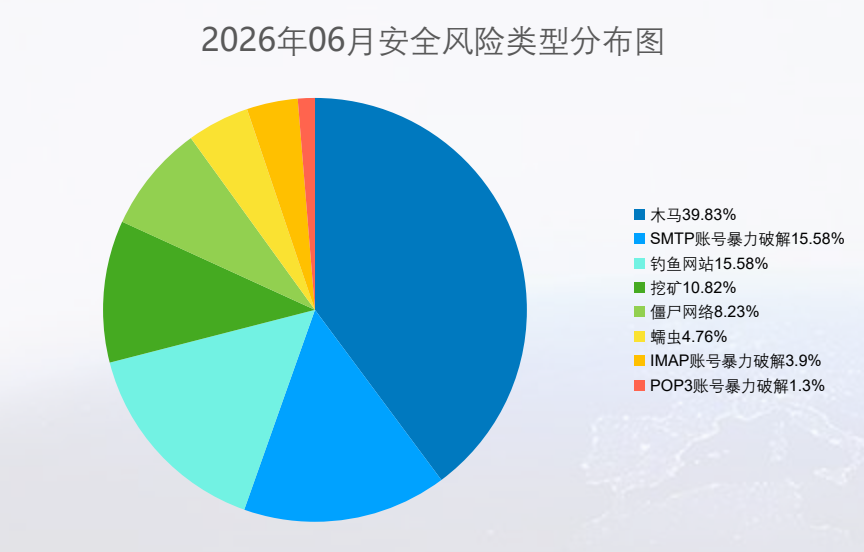
安全风险类型分布

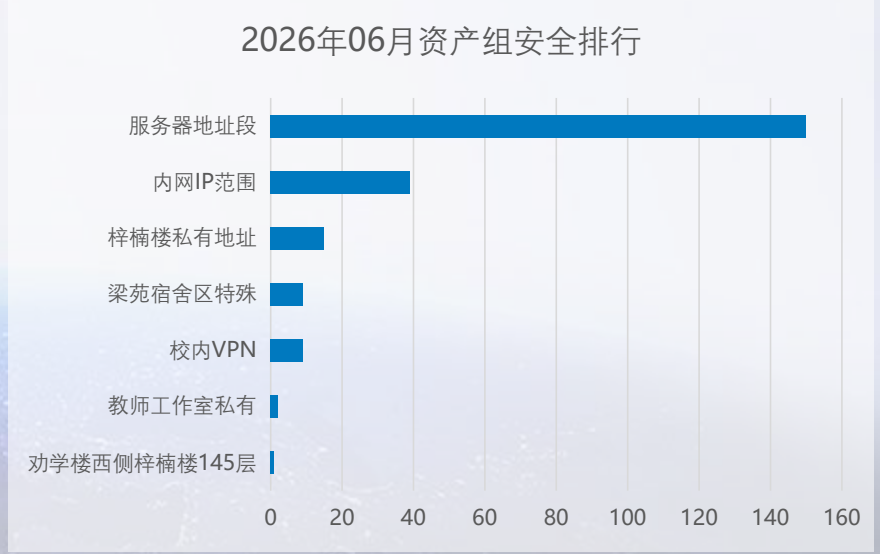
漏洞分布图

暂无数据

网络安全整体解读-安全总览

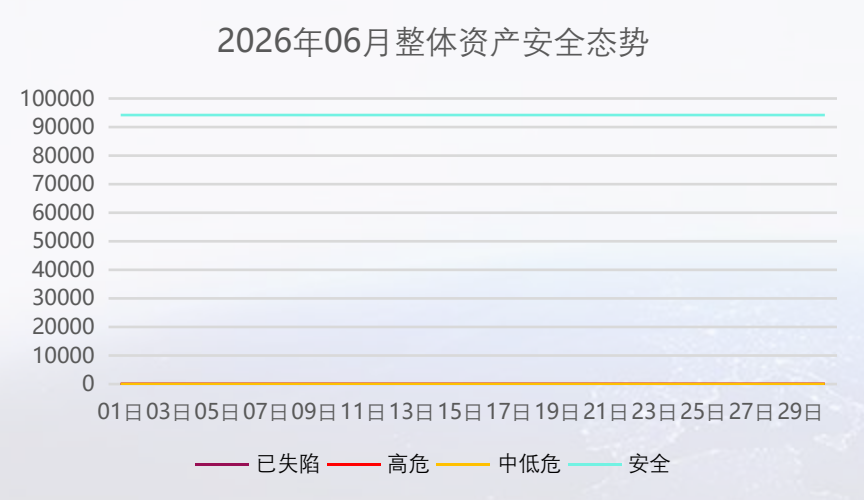
- 2026年06月最突出的安全风险前三名分别是木马、SMTP账号暴力破解、钓鱼网站，本月处理这三类风险分别为39.83%、15.58%、15.58%，占本月总风险71%；针对这些风险，共处置主机43个/次，处置漏洞0个；
- 按资产组分布，发生安全风险次数最多的是服务器地址段，共150次，占总数的64.94%；其次是内网IP范围（39次，16.88%）、梓楠楼私有地址（15次，6.49%）；安全风险次数最少的是校内VPN、教师工作室私有、劝学楼西侧梓楠楼145层。





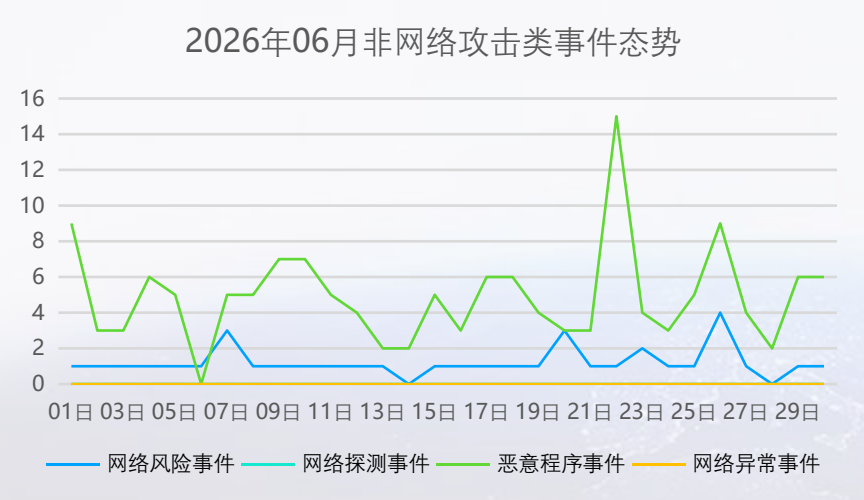
网络安全整体解读-安全态势

- 2026年06月平均每日捕获风险资产5.2个左右，占总资产数（服务器218个、终端93357个）0.01%；风险资产总数在6月9日达到高峰，共9个，占资产总数0.01%；“已失陷”资产在6月9日增幅最大，增幅达200%，从3个增加到9个；“已失陷”资产数在6月3日经过处置后，同比减少50%；“高危”资产数在6月8日经过处置后，同比减少100%；“安全”类资产在6月1日至6月3日、6月4日至6月6日等出现连续3日以上的持续增长；“安全”类资产在6月19日至6月22日、6月24日至6月26日等出现连续3日以上的持续减少；
- 2026年06月共捕获外部网络攻击2.12千万次，平均每日70.59万次；较上个月增加13.23%；在6月3日达到最高的83.11万次；波动最大的是6月20日，较6月19日减少60.48%；在6月1日至6月3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5日至6月7日、6月11日至6月14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

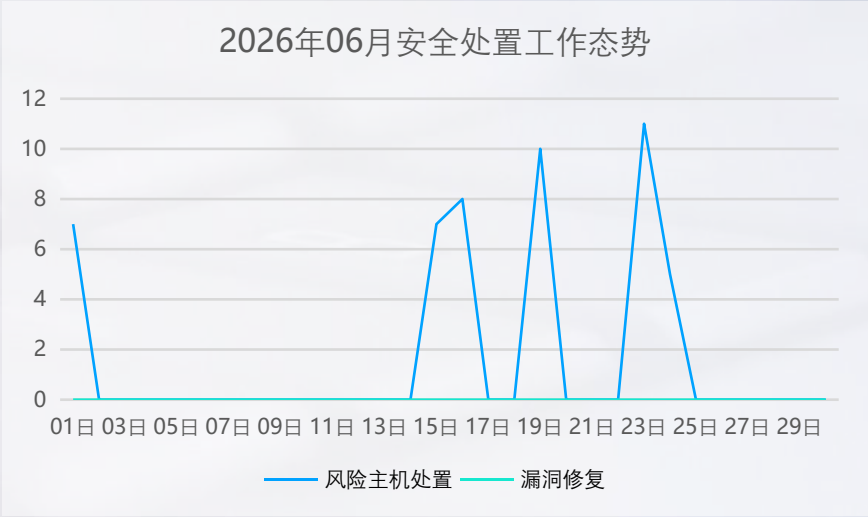
- 2026年06月共捕获有害程序、信息破坏、信息内容安全等其他非网络攻击类事件231次，日均7.7次，其中6月22日最高16次；
- 2026年06月共捕获漏洞0个，平均每日0个；捕获次数最高的是6月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；
- 其中高危漏洞0个，占比100%，平均每日0个；高危漏洞捕获次数最高的是6月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；



网络安全整体解读-安全处置工作概览

- 2026年06月共处置风险主机48个，较上个月增加6.67%；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	2.12千万次 ↑
修复漏洞	0次
处置主机	48条 ↑
合规检查	0次
重大活动保障	0次

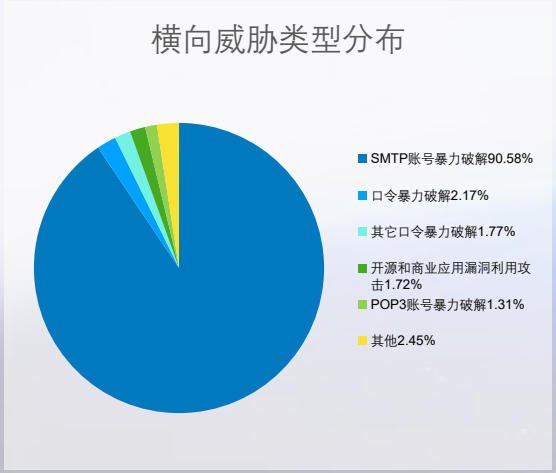


01 内部网络安全情况 - 网络安全风险详情

—— 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

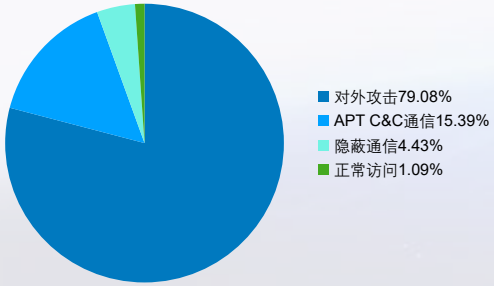
- 在2026年06月共捕获横向威胁主机757台，横向威胁事件62.88万件，其中SMTP账号暴力破解排名第一，占比90.58%；其次是口令暴力破解、其它口令暴力破解。
- 趋势上，平均每日发起横向威胁2.1万件；捕获次数最多的是6月29日，达4.22万次；波动最大的是6月25日，较6月24日增加117.93%；在6月6日至6月8日、6月13日至6月18日等出现连续3日以上的持续增长。在6月2日至6月6日、6月10日至6月13日出现连续3日以上的持续减少。
- 按资产组分布，发生横向威胁最多的是校内学院虚拟化机器，共51.87万次，占总数的82.5%；其次是锐捷交换机（6.23万次，9.9%）、内网IP范围（4.05万次，6.44%）等。



网络安全风险详情-外连威胁

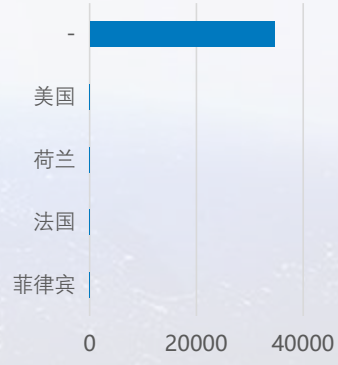
- 在2026年06月共捕获外连威胁主机180台，外连威胁事件4.1万件，其中对外攻击排名第一，占比79.08%；其次是APT C&C通信、隐蔽通信。
- 趋势上，平均每日发起外连威胁1367.8件；捕获次数最多的是6月5日，达3384次；波动最大的是6月6日，较6月5日减少65.54%；在6月18日至6月20日出现连续3日以上的持续增长。在6月5日至6月7日、6月26日至6月28日出现连续3日以上的持续减少。
- 风险主机外连地区既有境内也有境外；境外外连地区主要来自-、美国、荷兰、法国、菲律宾，这5个国家/地区的外连次数占总体境外外连地区的99.86%；境内主要来源辽宁、广东、浙江、北京、中国，这5个省份的外连次数占总体外连次数96.18%，占总外连次数的14.74%；

外连威胁类型分布



外连威胁趋势图

境外外连地区

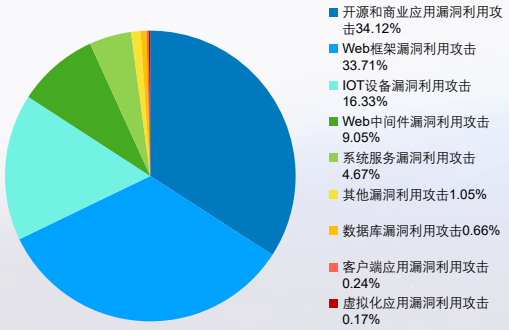


境内外连地区

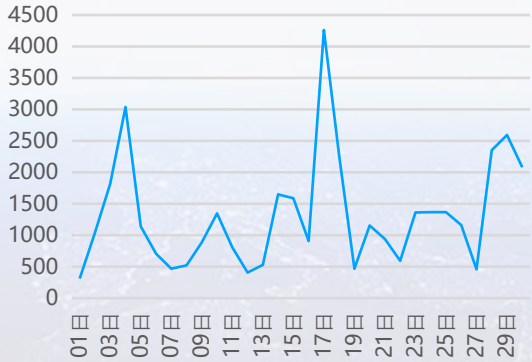
网络安全风险详情-漏洞利用

- 漏洞利用是最常见的一种网络攻击，2026年06月共捕获漏洞利用攻击告警3.96万次，其中开源和商业应用漏洞利用攻击排名第一，占比34.12%；其次是Web框架漏洞利用攻击、IOT设备漏洞利用攻击。
- 趋势上，平均每日发起漏洞利用攻击1319.83件；捕获次数最多的是6月17日，达4261次；波动最大的是6月28日，较6月27日增加412.42%；在6月1日至6月4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4日至6月7日、6月10日至6月12日等出现连续3日以上的持续减少。
- 按资产组分布，发生漏洞利用攻击最多的是服务器地址段，共1.34万次，占总数的40.03%；其次是校内学院虚拟化机器（1.23万次，36.74%）、内网IP范围（3536次，10.54%）等。

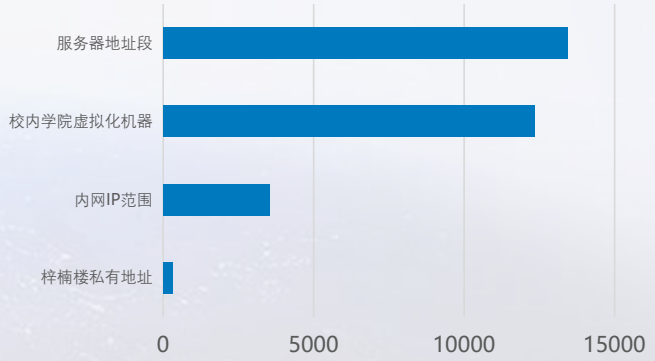
漏洞利用攻击类型



漏洞利用趋势图

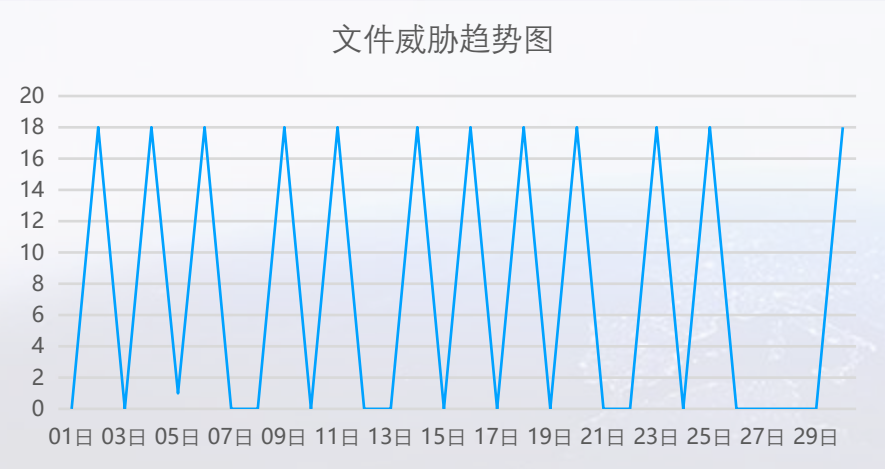


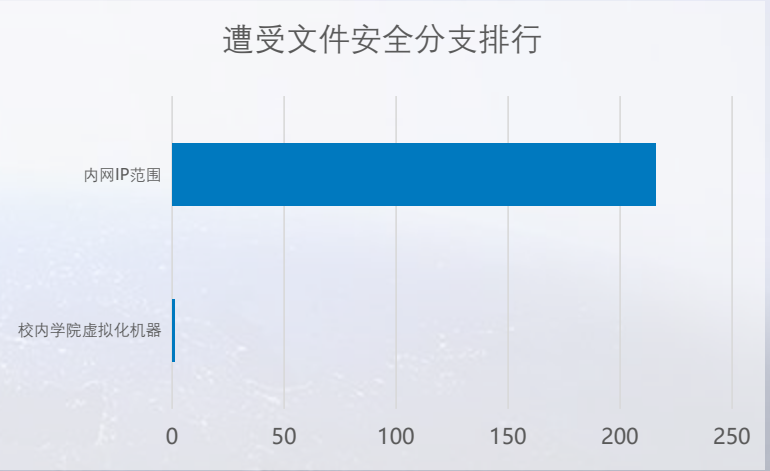
遭受漏洞利用攻击分支排行



网络安全风险详情-文件安全

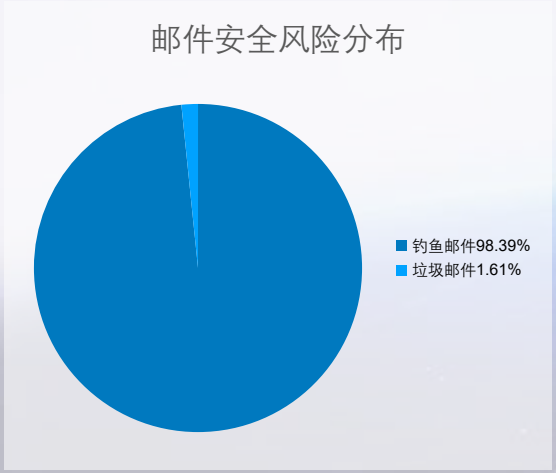
- 文件是病毒传播的常见手段；2026年06月共查杀文件1327967余次，确认为恶意文件的有217个；
- 趋势上，平均每日捕获恶意文件7.23件；审计次数最多的是6月2日，达18次；波动最大的是6月3日，较6月2日减少100%；
- 按资产组分布，发生文件安全最多的是内网IP范围，共216次，占总数的99.54%；其次是校内学院虚拟化机器（1次，0.46%）等。

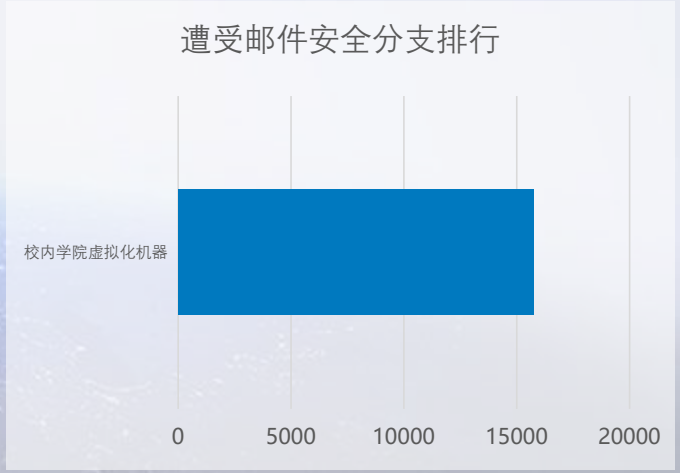




网络安全风险详情-邮件安全

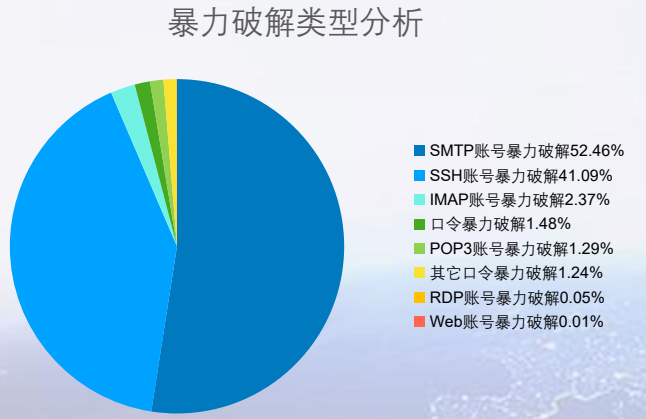
- 邮件是恶意软件分发和网络钓鱼的头号媒介；2026年06月，共捕获钓鱼邮件98.39%15485次；垃圾邮件1.61%254次；
- 趋势上，平均每日捕获邮件安全风险524.63件；捕捉最高的是6月26日，达966次；波动最大的是6月15日，较6月14日增加6500%；在6月7日至6月9日、6月14日至6月16日等出现连续3日以上的持续增长。在6月1日至6月4日、6月5日至6月7日等出现连续3日以上的持续减少。
- 按资产组分布，发生邮件安全最多的是校内学院虚拟化机器，共1.57万次，占总数的100%；





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06月共捕获暴力破解攻击告警33.05万次，其中SMTP账号暴力破解排名第一，占比52.46%;其次是SSH账号暴力破解、IMAP账号暴力破解。
- 暴破频率最高达1801次/分钟，该告警于2026年06月13日01时38分捕获，来自于挪威攻击者193.90.12.40攻击校内学院虚拟化机器的服务器202.199.162.34



捕获时间：	2026-06-13 01:38:15
攻击者：	193.90.12.40（挪威）
攻击手段：	账号暴力破解
暴破频率：	最高达1801次/分钟
受害者：	校内学院虚拟化机器（202.199.162.34）

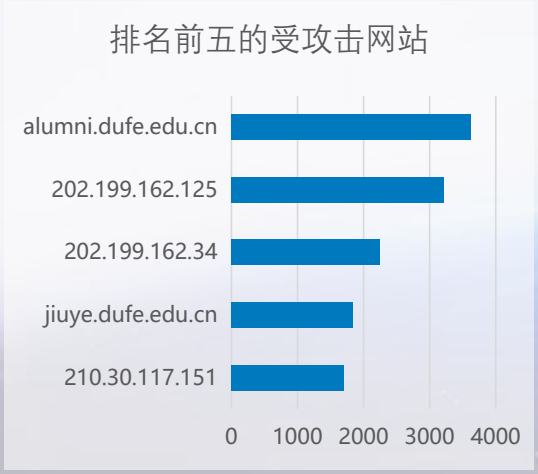
网络安全风险详情-业务脆弱性

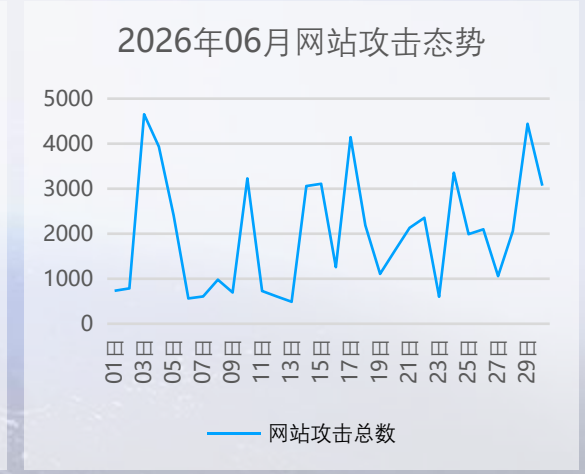
- 业务脆弱性是指“资产中能被威胁所利用的弱点”，包括技术层面的脆弱性，如：漏洞、WEB明文传输、配置错误，还有管理层面的风险，如：弱密码。2026年06月共捕获漏洞0个，Web明文传输175个，配置错误风险282个，弱密码账号141个；
- 捕获最多的是-，共捕获0次，占所有漏洞的0%；
- 平均每日捕获高危漏洞0个；捕获次数最多的是6月1日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；

0个	175个	282个	141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

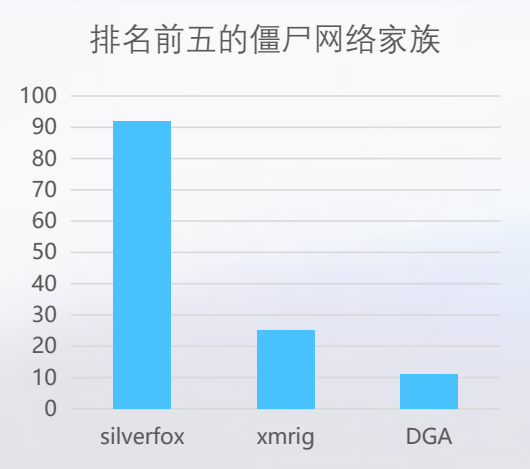
- 2026年06月，共捕获网站类攻击6.01万次，其中被攻击最多的网站是alumni.dufe.edu.cn，达到3623次，占总体的6.03%；其次是202.199.162.125、202.199.162.34。
- 2026年06月捕获的网站攻击中，既有来自境内的，也有来自境外的；境外攻击源主要来自美国、新加坡、德国、加拿大、英国，这5个国家/地区的网站攻击占总体境外网站攻击的60.3%；境内主要来源辽宁、香港、北京、江苏、浙江，这5个省份的网站攻击占总体境内网站攻击68.9%，占所有网站攻击的33.04%；
- 趋势上，平均每日捕获网络攻击2001.87次；捕获次数最高的是6月3日，达4652次；波动最大的是6月14日，较6月13日增加525.56%；在6月1日至6月3日、6月6日至6月8日等出现连续3日以上的持续增长。在6月3日至6月6日、6月10日至6月13日等出现连续3日以上的持续减少。

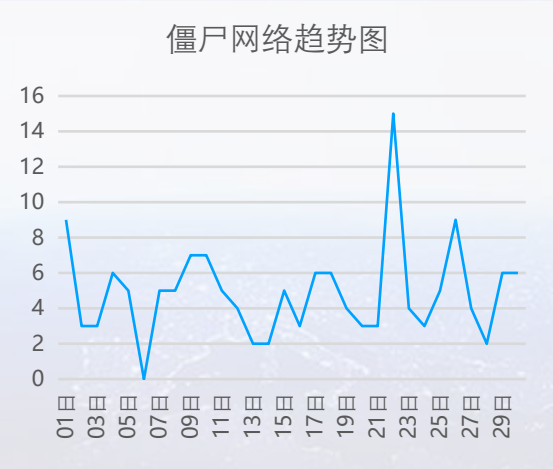


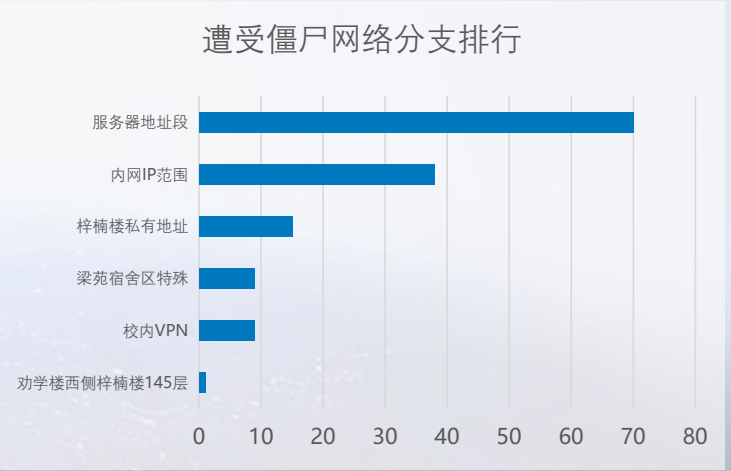


网络安全风险详情-僵尸网络

- 2026年06月，共捕获僵尸网络147次；其中silverfox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62.59%；排名第二第三的xmrig、DGA比例分别为17.01%、7.48%
- 趋势上，平均每日捕获僵尸网络攻击4.9次；捕获次数最高的是6月22日，达15次；波动最大的是6月22日，较6月21日增加400%；在6月24日至6月26日出现连续3日以上的持续增长。在6月4日至6月6日、6月10日至6月13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70次，占总数的47.62%；其次是内网IP范围（38次，25.85%）、梓楠楼私有地址（15次，10.2%）等。

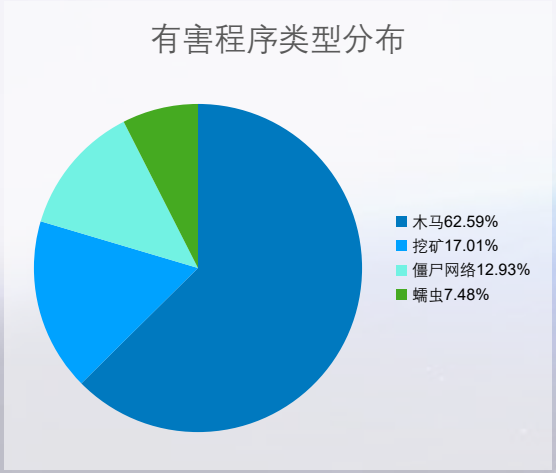


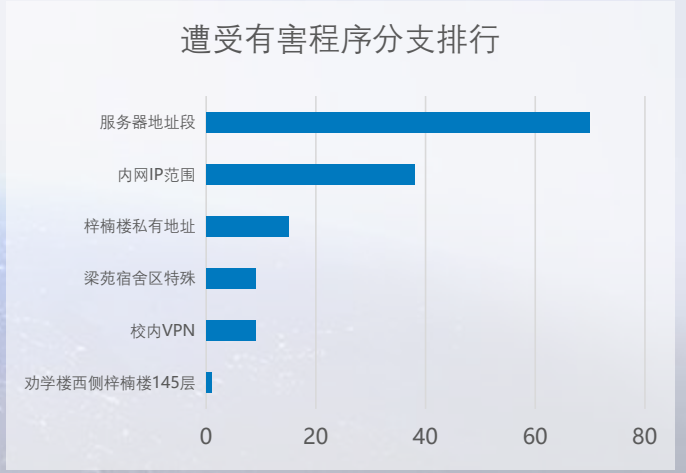




网络安全风险详情-有害程序

- 2026年06月，共捕获有害程序告警147次；其中最为活跃的是木马，共捕获92次，占所有恶意程序捕获数量的62.59%；而排名第二第三的挖矿、僵尸网络的比例分别为17.01%、12.93%
- 趋势上，平均每日捕获有害程序风险4.9次；捕获次数最高的是6月22日，达15次；波动最大的是6月22日，较6月21日增加400%；在6月24日至6月26日出现连续3日以上的持续增长。在6月4日至6月6日、6月10日至6月13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70次，占总数的47.62%；其次是内网IP范围（38次，25.85%）、梓楠楼私有地址（15次，10.2%）等。





THANK YOU

2026年06月