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07月

目录 CONTENTS

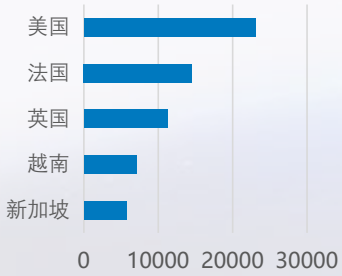
01 内部网络安全情况 - 网络安全整体解读

网络安全整体解读-安全总览

- 共捕获攻击次数2.06千万次,较上个月减少2.89%；平均每日捕获攻击近66.34万次，攻击者数量达9.77万个，来源国家或地区184个，境外主要来自美国、法国、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214次；网络攻击事件52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24个；

2.06千万次	9.77万个	150个	214个	52个	8个	0个	24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

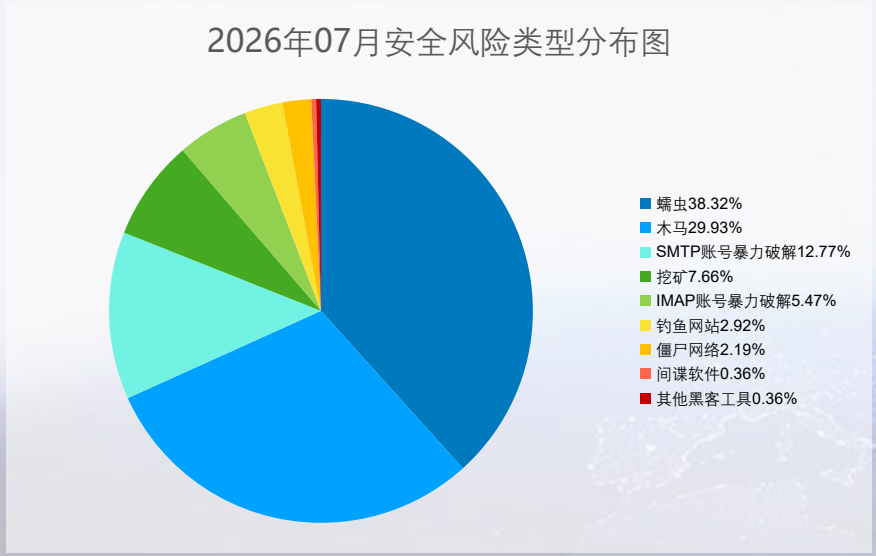
安全风险类型分布

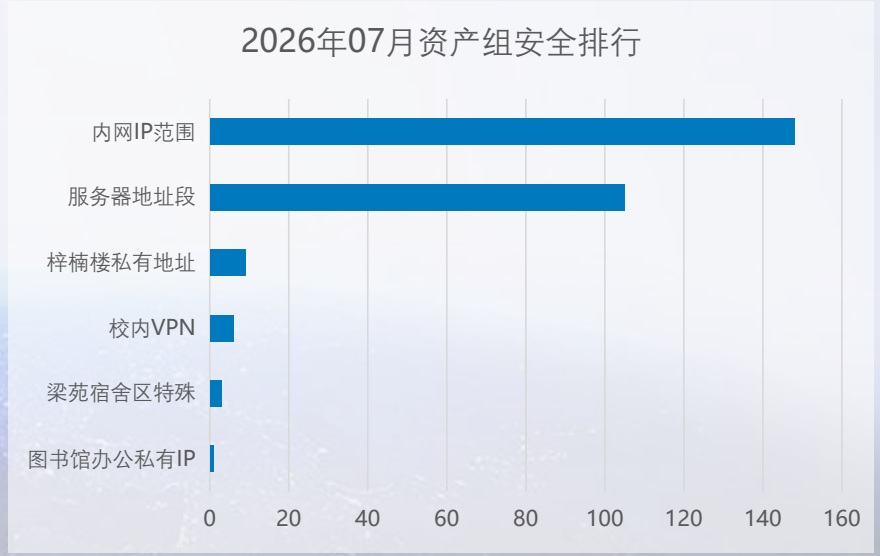
漏洞分布图

暂无数据

网络安全整体解读-安全总览

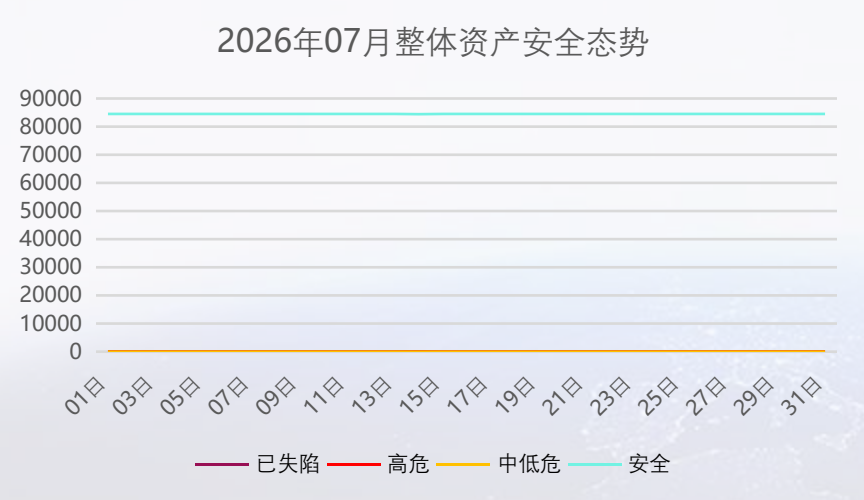
- 2026年07月最突出的安全风险前三名分别是蠕虫、木马、SMTP账号暴力破解，本月处理这三类风险分别为38.32%、29.93%、12.77%，占本月总风险81.02%；针对这些风险，共处置主机94个/次，处置漏洞0个；
- 按资产组分布，发生安全风险次数最多的是内网IP范围，共148次，占总数的54.01%；其次是服务器地址段（105次，38.32%）、梓楠楼私有地址（9次，3.28%）；安全风险次数最少的是校内VPN、梁苑宿舍区特殊、图书馆办公私有IP。





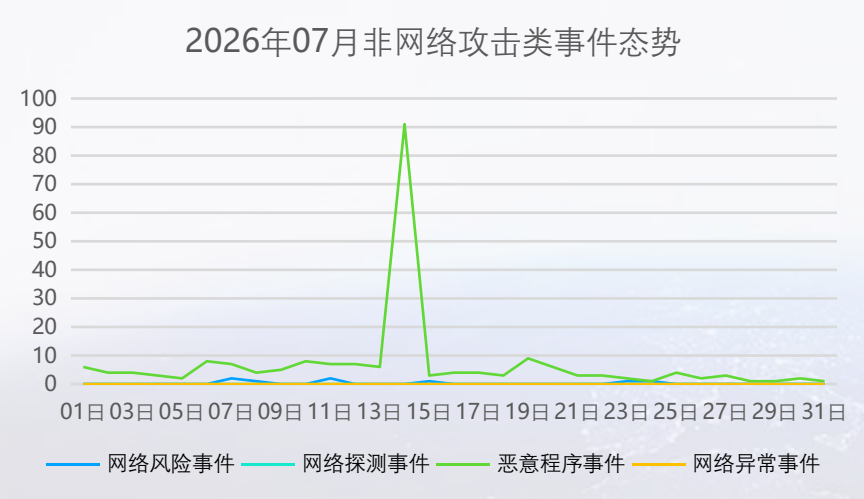
网络安全整体解读-安全态势

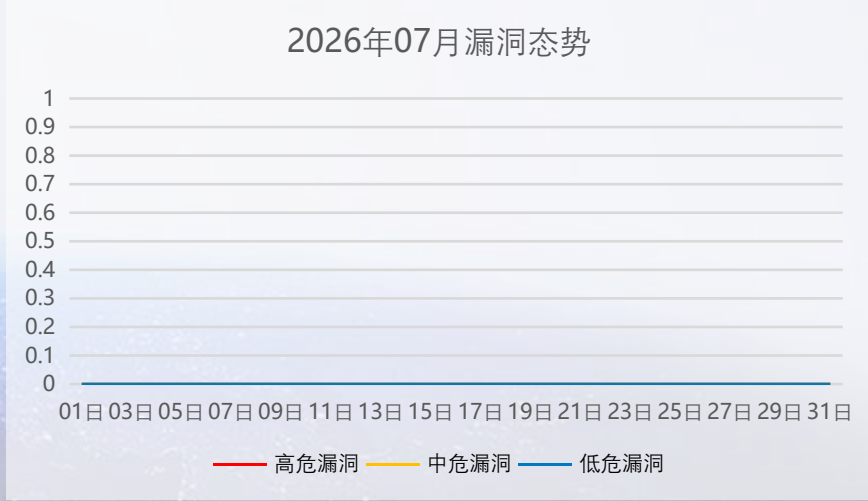
- 2026年07月平均每日捕获风险资产7.1个左右，占总资产数（服务器217个、终端83688个）0.01%；风险资产总数在7月14日达到高峰，共89个，占资产总数0.11%；“已失陷”资产在7月14日增幅最大，增幅达4350%，从2个增加到89个；“已失陷”资产数在7月15日经过处置后，同比减少94.38%；“高危”资产数在7月8日经过处置后，同比减少100%；“安全”类资产在7月3日至7月5日、7月6日至7月8日等出现连续3日以上的持续增长；“安全”类资产在7月8日至7月11日、7月27日至7月29日出现连续3日以上的持续减少；
- 2026年07月共捕获外部网络攻击2.06千万次，平均每日66.34万次；较上个月减少2.89%；在7月14日达到最高的76.01万次；按日同比未出现20%以上的波动，总体趋势比较平稳；在7月6日至7月9日、7月25日至7月29日出现连续3日以上的持续增长。在7月4日至7月6日、7月11日至7月13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07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274次，日均8.84次，其中7月14日最高91次；
- 2026年07月共捕获漏洞0个，平均每日0个；捕获次数最高的是7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7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；

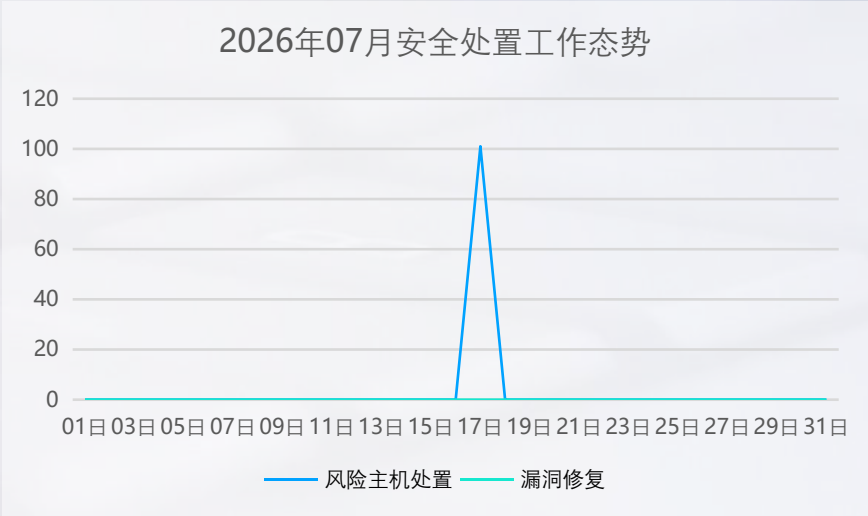




网络安全整体解读-安全处置工作概览

- 2026年07月共处置风险主机101个，较上个月增加110.42%；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	2.06千万次
修复漏洞	0次
处置主机	101条
合规检查	0次
重大活动保障	0次

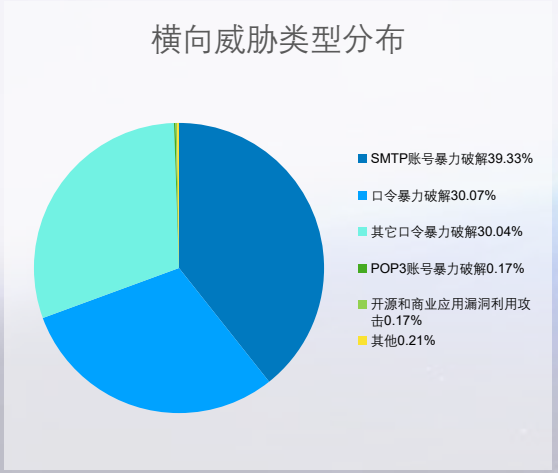


01 内部网络安全情况 - 网络安全风险详情

—— 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

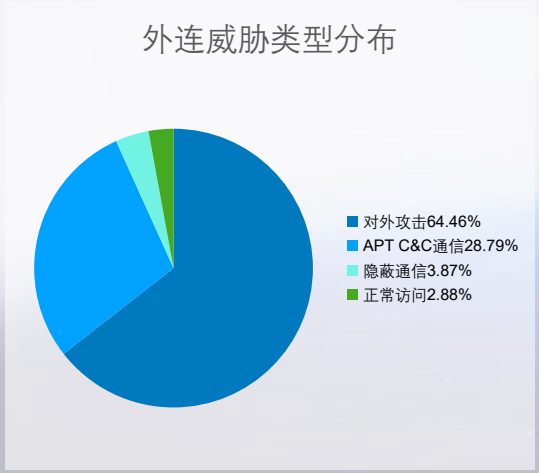
网络安全风险详情-横向威胁

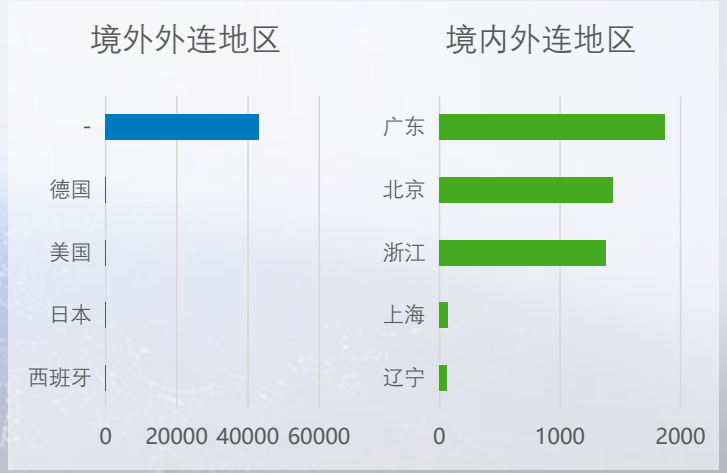
- 在2026年07月共捕获横向威胁主机681台，横向威胁事件2.48百万件，其中SMTP账号暴力破解排名第一，占比39.33%；其次是口令暴力破解、其它口令暴力破解。
- 趋势上，平均每日发起横向威胁8.01万件；捕获次数最多的是7月30日，达40.7万次；波动最大的是7月19日，较7月18日增加1187.41%；在7月4日至7月6日、7月11日至7月14日等出现连续3日以上的持续增长。在7月2日至7月4日、7月14日至7月16日等出现连续3日以上的持续减少。
- 按资产组分布，发生横向威胁最多的是校内学院虚拟化机器，共2.36百万次，占总数的95.03%；其次是锐捷交换机（7.01万次，2.82%）、内网IP范围（4.97万次，2%）等。



网络安全风险详情-外连威胁

- 在2026年07月共捕获外连威胁主机153台，外连威胁事件4.82万件，其中对外攻击排名第一，占比64.46%；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1554.81件；捕获次数最多的是7月14日，达4256次；波动最大的是7月14日，较7月13日增加190.91%；在7月11日至7月14日、7月17日至7月20日等出现连续3日以上的持续增长。在7月2日至7月5日、7月20日至7月23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-、德国、美国、日本、西班牙，这5个国家/地区的外连次数占总体境外外连地区的99.98%；境内主要来源广东、北京、浙江、上海、辽宁，这5个省份的外连次数占总体外连次数95.53%，占总外连次数的10.01%；

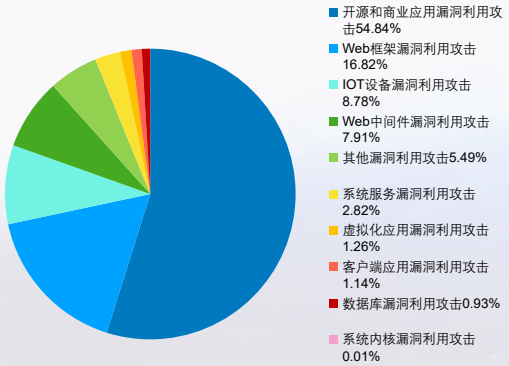




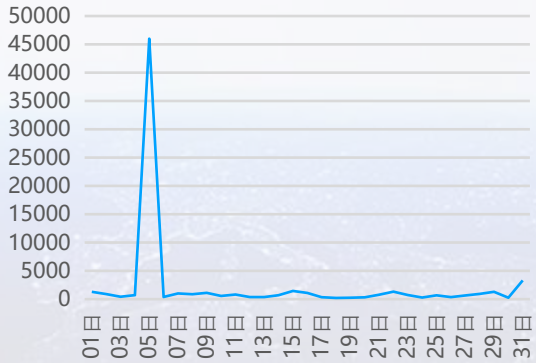
网络安全风险详情-漏洞利用

- 漏洞利用是最常见的一种网络攻击，2026年07月共捕获漏洞利用攻击告警6.98万次，其中开源和商业应用漏洞利用攻击排名第一，占比54.84%；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2251.71件；捕获次数最多的是7月5日，达4.6万次；波动最大的是7月6日，较7月5日减少99.16%；在7月3日至7月5日、7月13日至7月15日等出现连续3日以上的持续增长。在7月1日至7月3日、7月11日至7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57.88%；其次是校内学院虚拟化机器（4609次，19.98%）、内网IP范围（4205次，18.23%）等。

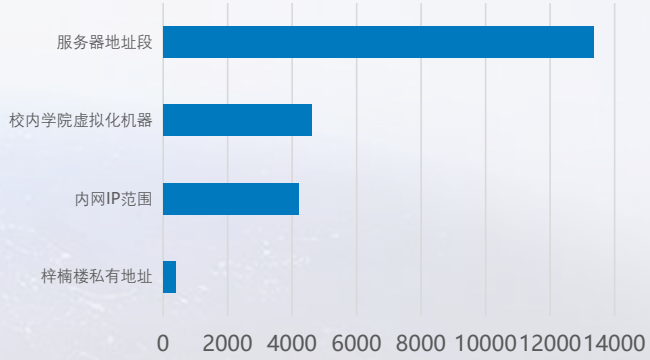
漏洞利用攻击类型



漏洞利用趋势图

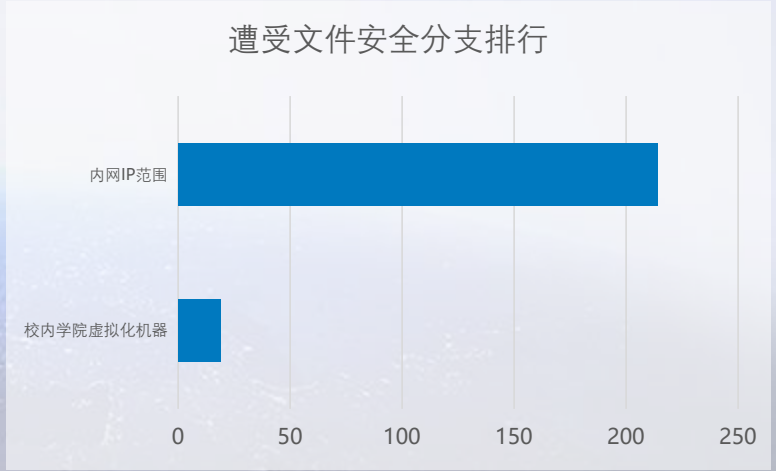


遭受漏洞利用攻击分支排行



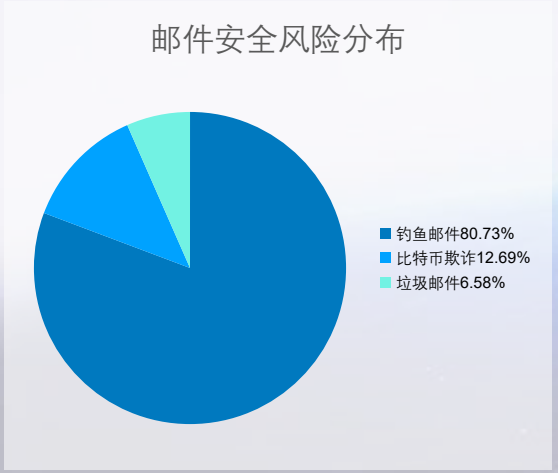
网络安全风险详情-文件安全

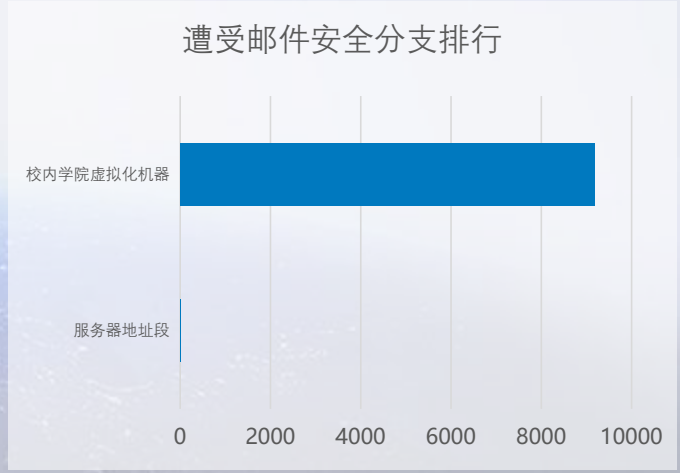
- 文件是病毒传播的常见手段；2026年07月共查杀文件692236余次，确认为恶意文件的有236个；
- 趋势上，平均每日捕获恶意文件7.61件；审计次数最多的是7月7日，达34次；波动最大的是7月3日，较7月2日减少100%；在7月26日至7月28日出现连续3日以上的持续增长。
- 按资产组分布，发生文件安全最多的是内网IP范围，共214次，占总数的90.68%；其次是校内学院虚拟化机器（19次，8.05%）等。



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07月，共捕获钓鱼邮件80.73%7420次；比特币欺诈12.69%1166次；垃圾邮件6.58%605次；
- 趋势上，平均每日捕获邮件安全风险296.48件；捕捉最高的是7月7日，达1210次；波动最大的是7月29日，较7月28日增加660%；在7月3日至7月7日、7月15日至7月18日等出现连续3日以上的持续增长。在7月1日至7月3日、7月7日至7月15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9190次，占总数的99.99%；其次是服务器地址段（1次，0.01%）等。

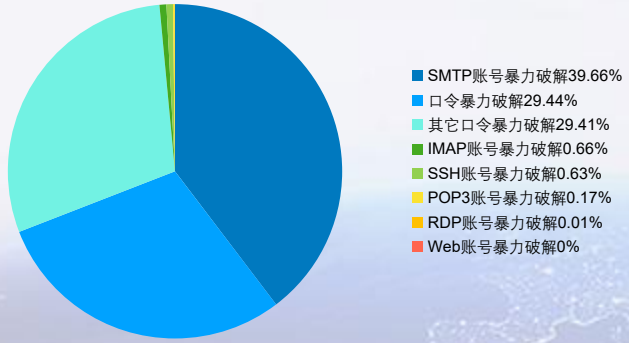




网络安全风险详情-暴力破解

- 暴力破解是最常见的一种网络攻击，2026年07月共捕获暴力破解攻击告警1.98百万次，其中SMTP账号暴力破解排名第一，占比39.66%;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07月01日19时49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202.199.162.124

暴力破解类型分析



捕获时间：	2026-07-01 19:49:46
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（202.199.162.124）

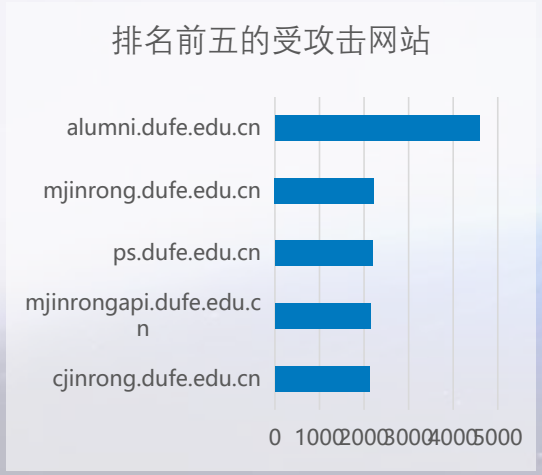
网络安全风险详情-业务脆弱性

- 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07月共捕获漏洞0个，Web明文传输167个，配置错误风险284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7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	167个	284个	82个
漏洞	Web明文传输	配置风险	弱密码

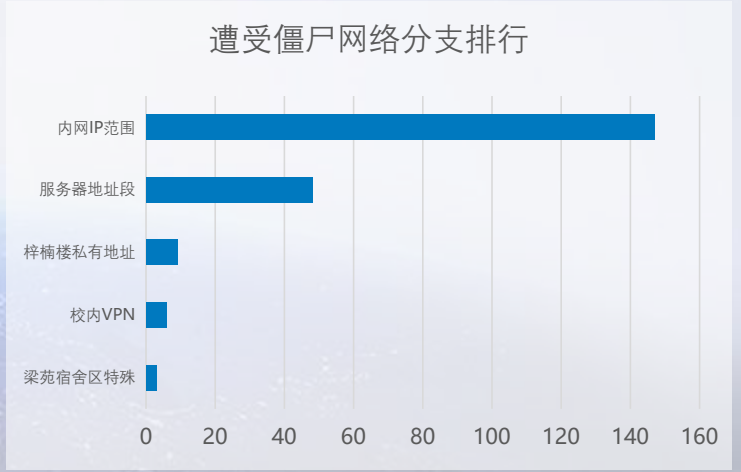
网络安全风险详情-网站攻击

- 2026年07月，共捕获网站类攻击4.7万次，其中被攻击最多的网站是alumni.dufe.edu.cn，达到4592次，占总体的9.77%；其次是mjinrong.dufe.edu.cn、ps.dufe.edu.cn。
- 2026年07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、新加坡、巴西、德国，这5个国家/地区的网站攻击占总体境外网站攻击的59.89%；境内主要来源辽宁、浙江、香港、北京、江苏，这5个省份的网站攻击占总体境内网站攻击87.76%，占所有网站攻击的56.81%；
- 趋势上，平均每日捕获网络攻击1516.61次；捕获次数最高的是7月5日，达9755次；波动最大的是7月6日，较7月5日减少91.62%；在7月3日至7月5日、7月19日至7月22日等出现连续3日以上的持续增长。在7月1日至7月3日、7月5日至7月7日等出现连续3日以上的持续减少。



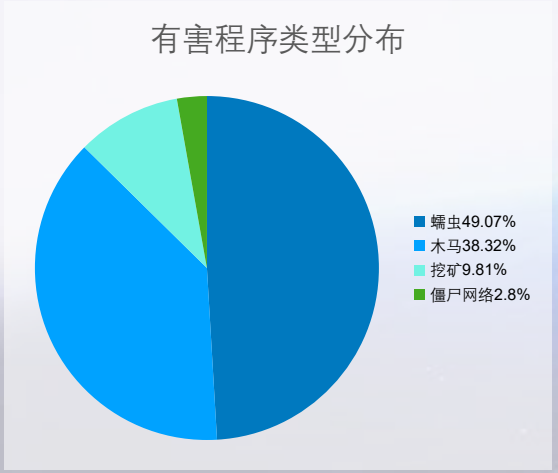
网络安全风险详情-僵尸网络

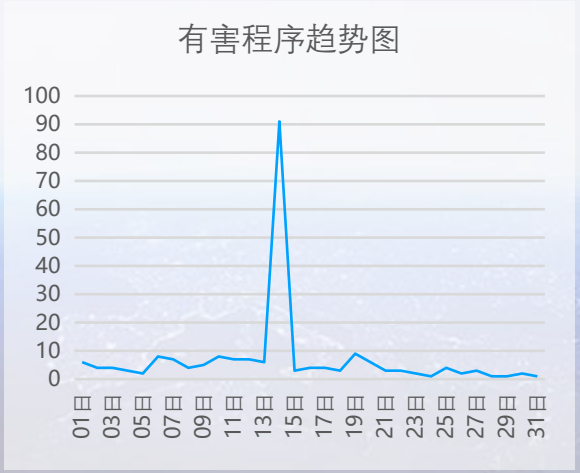
- 2026年07月，共捕获僵尸网络214次；其中xred家族是攻击态势最为活跃的僵尸网络家族，占所有僵尸网络拦截数量的49.07%；排名第二的silverfox比例为38.32%
- 趋势上，平均每日捕获僵尸网络攻击6.9次；捕获次数最高的是7月14日，达91次；波动最大的是7月15日，较7月14日减少96.7%；在7月8日至7月10日出现连续3日以上的持续增长。在7月3日至7月5日、7月6日至7月8日等出现连续3日以上的持续减少。
- 按资产组分布，发生僵尸网络最多的是内网IP范围，共147次，占总数的68.69%；其次是服务器地址段（48次，22.43%）、梓楠楼私有地址（9次，4.21%）等。

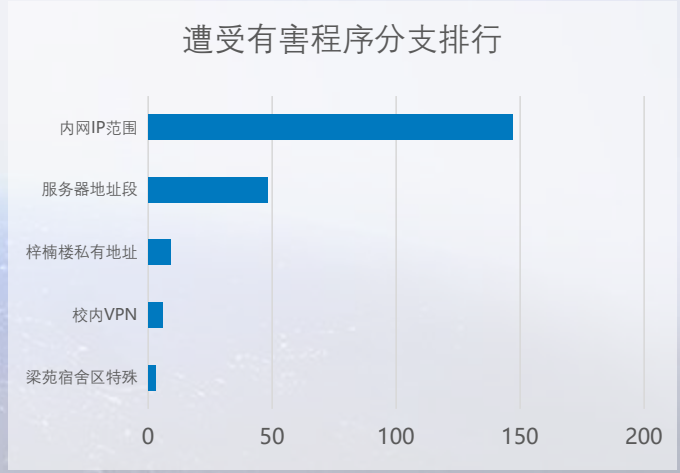


网络安全风险详情-有害程序

- 2026年07月，共捕获有害程序告警214次；其中最为活跃的是蠕虫，共捕获105次，占所有恶意程序捕获数量的49.07%；而排名第二第三的木马、挖矿的比例分别为38.32%、9.81%
- 趋势上，平均每日捕获有害程序风险6.9次；捕获次数最高的是7月14日，达91次；波动最大的是7月15日，较7月14日减少96.7%；在7月8日至7月10日出现连续3日以上的持续增长。在7月3日至7月5日、7月6日至7月8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内网IP范围，共147次，占总数的68.69%；其次是服务器地址段（48次，22.43%）、梓楠楼私有地址（9次，4.21%）等。







THANK YOU

2026年07月