网络安全态势月报

智慧校园建设中心

2026年03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3.74百万次,较上个月增加48.62%；平均每日捕获攻击近12.08万次，攻击者数量达1.37万个，来源国家或地区128个，境外主要来自加拿大、荷兰、美国，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188次；网络风险事件33次；未发生网络探测事件、网络异常事件；
- 共捕获漏洞1个；弱密码30个；

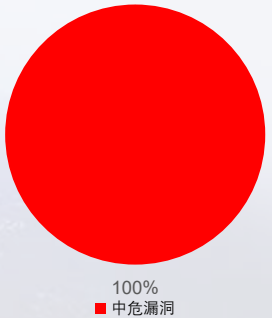
3.74百万次	1.37万个	94个	188个	33个	9个	1个	30个
攻击总数	攻击者	境外攻击地区	恶意程序事件	网络风险事件	其他	漏洞总数	弱密码账号

境外攻击源地区

境内攻击源地区

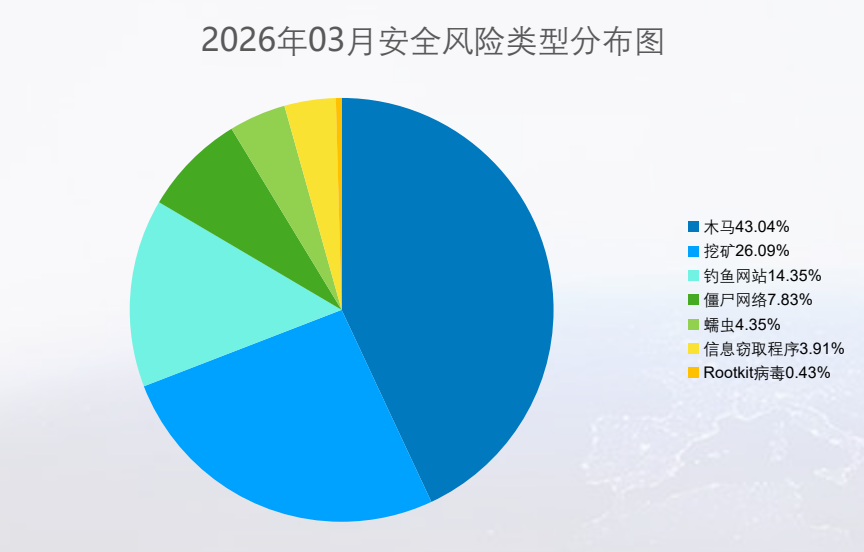
安全风险类型分布

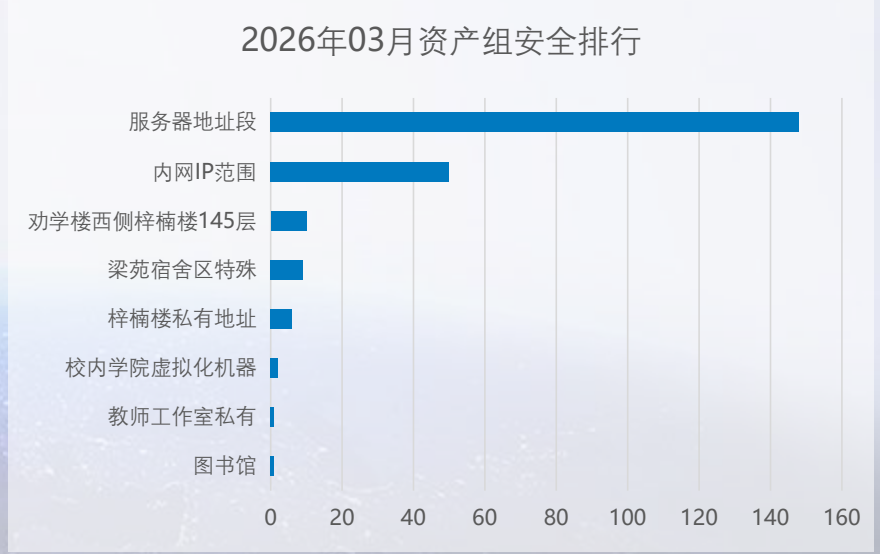
漏洞分布图



网络安全整体解读-安全总览

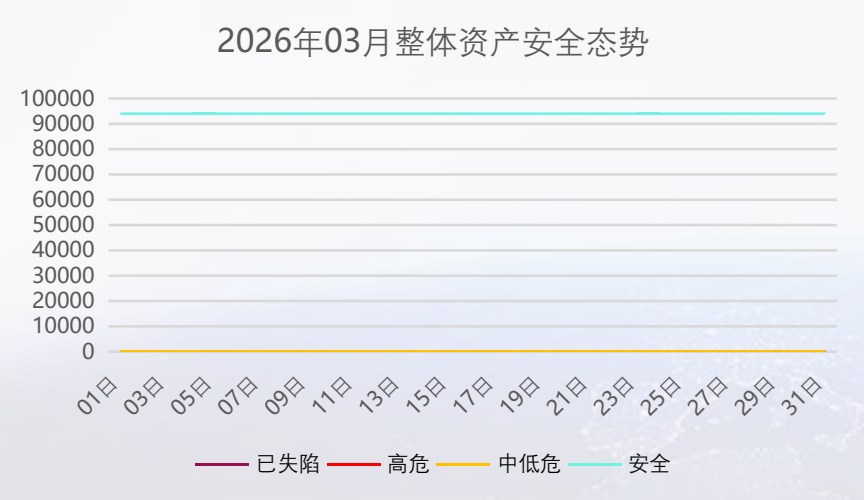
- 2026年03月最突出的安全风险前三名分别是木马、挖矿、钓鱼网站，本月处理这三类风险分别为43.04%、26.09%、14.35%，占本月总风险83.48%；针对这些风险，共处置主机74个/次，处置漏洞0个；
- 按资产组分布，发生安全风险次数最多的是服务器地址段，共148次，占总数的64.35%；其次是内网IP范围（50次，21.74%）、劝学楼西侧梓楠楼145层（10次，4.35%）；安全风险次数最少的是校内学院虚拟化机器、教师工作室私有、图书馆。





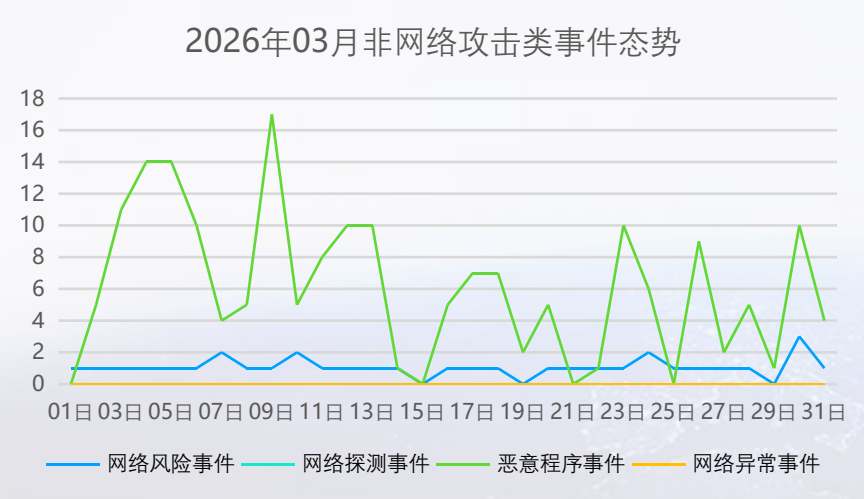
网络安全整体解读-安全态势

- 2026年03月平均每日捕获风险资产4.06个左右，占总资产数（服务器292个、终端93150个）0%；风险资产总数在3月4日达到高峰，共7个，占资产总数0.01%；“已失陷”资产在3月26日增幅最大，增幅达400%，从1个增加到5个；“已失陷”资产数在3月15日经过处置后，同比减少100%；“高危”资产数在3月8日经过处置后，同比减少100%；“安全”类资产在3月5日至3月8日、3月12日至3月15日等出现连续3日以上的持续增长；“安全”类资产在3月1日至3月4日、3月10日至3月12日等出现连续3日以上的持续减少；
- 2026年03月共捕获外部网络攻击3.74百万次，平均每日12.08万次；较上个月增加48.62%；在3月25日达到最高的22.41万次；波动最大的是3月4日，较3月3日增加174.17%；在3月8日至3月11日、3月15日至3月18日等出现连续3日以上的持续增长。在3月6日至3月8日、3月13日至3月15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

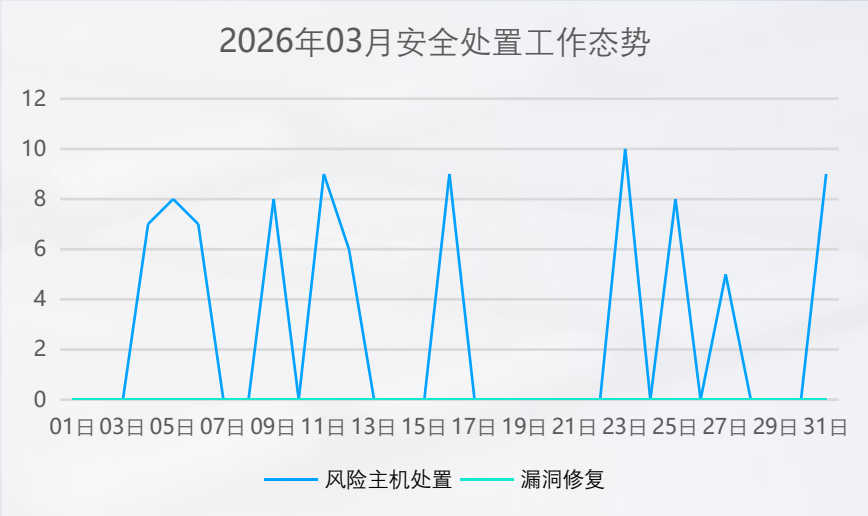
- 2026年03月共捕获有害程序、信息破坏、信息内容安全等其他非网络攻击类事件230次，日均7.42次，其中3月9日最高18次；
- 2026年03月共捕获漏洞1个，平均每日0.03个；捕获次数最高的是3月27日，达1个；按日同比，在3月28日经过加固后；同比减少100%；
- 其中高危漏洞0个，占比0%，平均每日0个；高危漏洞捕获次数最高的是0月0日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；



网络安全整体解读-安全处置工作概览

- 2026年03月共处置风险主机86个，较上个月增加126.32%；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	3.74百万次
修复漏洞	0次
处置主机	86条
合规检查	0次
重大活动保障	0次



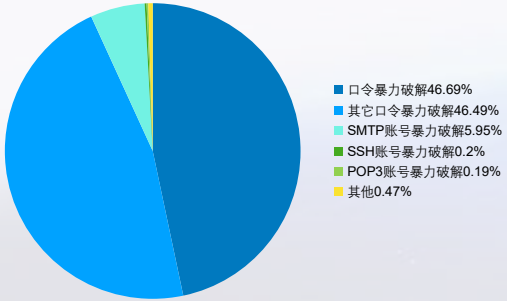
01 内部网络安全情况 - 网络安全风险详情

—— 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

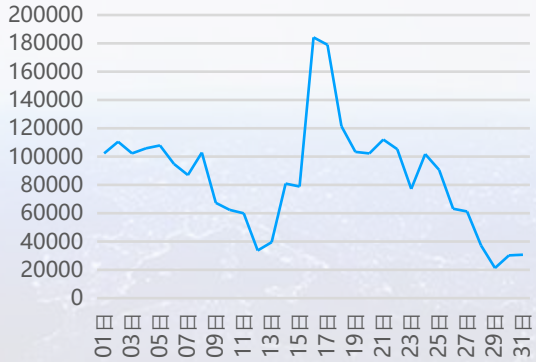
网络安全风险详情-横向威胁

- 在2026年03月共捕获横向威胁主机786台，横向威胁事件2.66百万件，其中口令暴力破解排名第一，占比46.69%；其次是其它口令暴力破解、SMTP账号暴力破解。
- 趋势上，平均每日发起横向威胁8.57万件；捕获次数最多的是3月16日，达18.42万次；波动最大的是3月16日，较3月15日增加133.52%；在3月3日至3月5日、3月12日至3月14日等出现连续3日以上的持续增长。在3月5日至3月7日、3月8日至3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2.53百万次，占总数的95.19%；其次是锐捷交换机（6.63万次，2.5%）、内网IP范围（4.91万次，1.85%）等。

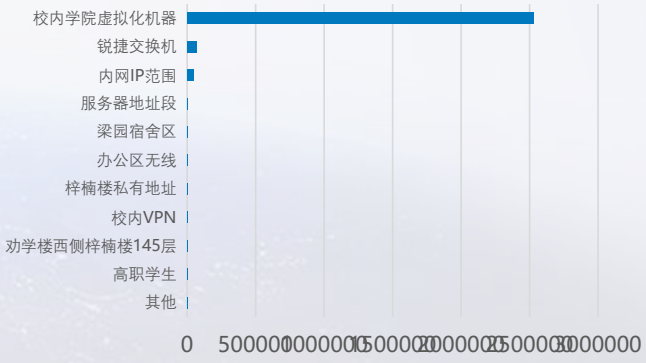
横向威胁类型分布



横向威胁趋势图

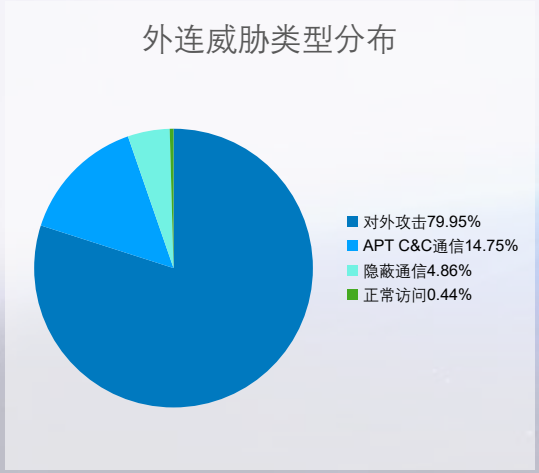


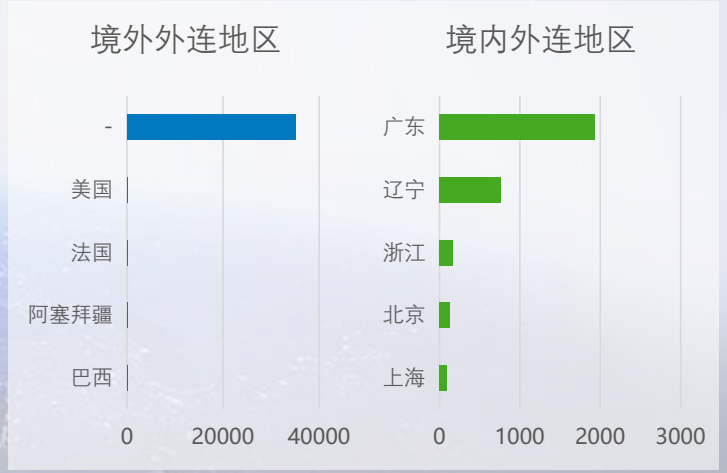
遭受横向威胁分支排行



网络安全风险详情-外连威胁

- 在2026年03月共捕获外连威胁主机167台，外连威胁事件3.88万件，其中对外攻击排名第一，占比79.95%；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1251.16件；捕获次数最多的是3月10日，达2193次；波动最大的是3月10日，较3月9日增加43.33%；在3月1日至3月3日、3月4日至3月7日等出现连续3日以上的持续增长。在3月10日至3月14日、3月18日至3月22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-、美国、法国、阿塞拜疆、巴西，这5个国家/地区的外连次数占总体境外外连地区的99.94%；境内主要来源广东、辽宁、浙江、北京、上海，这5个省份的外连次数占总体外连次数87.18%，占总外连次数的7.96%；

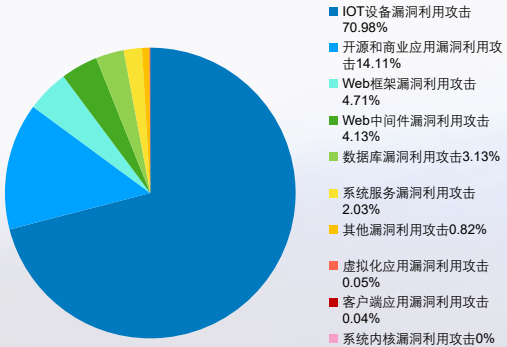




网络安全风险详情-漏洞利用

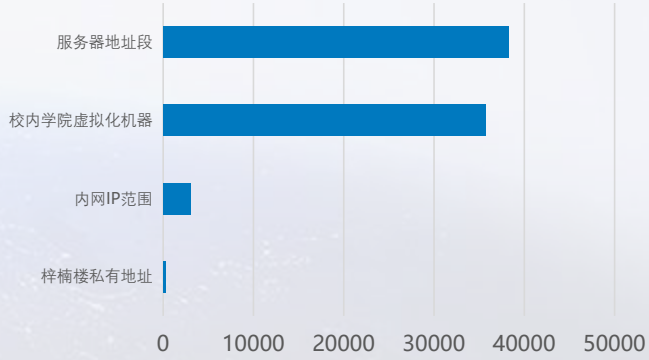
- 漏洞利用是最常见的一种网络攻击，2026年03月共捕获漏洞利用攻击告警9.09万次，其中IOT设备漏洞利用攻击排名第一，占比70.98%；其次是开源和商业应用漏洞利用攻击、Web框架漏洞利用攻击。
- 趋势上，平均每日发起漏洞利用攻击2932.39件；捕获次数最多的是3月17日，达5.28万次；波动最大的是3月17日，较3月16日增加5150.05%；在3月1日至3月4日、3月12日至3月14日等出现连续3日以上的持续增长。在3月6日至3月8日、3月17日至3月19日等出现连续3日以上的持续减少。
- 按资产组分布，发生漏洞利用攻击最多的是服务器地址段，共3.83万次，占总数的44.15%；其次是校内学院虚拟化机器（3.57万次，41.21%）、内网IP范围（3074次，3.55%）等。

漏洞利用攻击类型



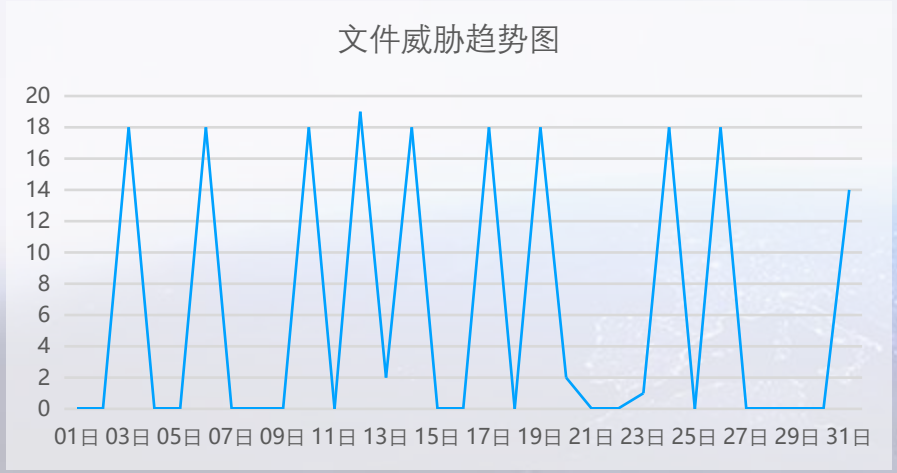
漏洞利用趋势图

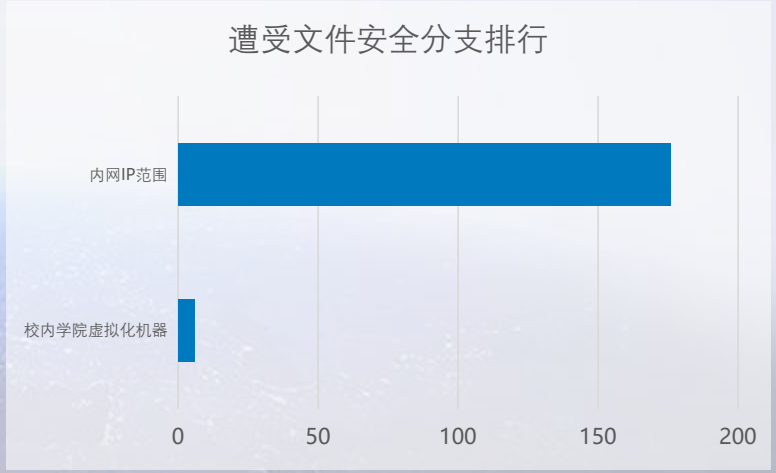
遭受漏洞利用攻击分支排行



网络安全风险详情-文件安全

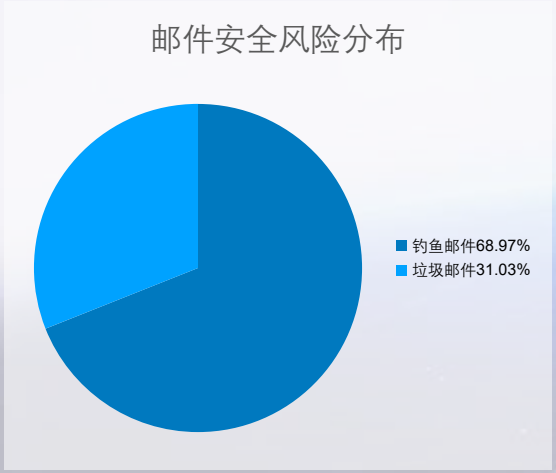
- 文件是病毒传播的常见手段；2026年03月共查杀文件926085余次，确认为恶意文件的有182个；
- 趋势上，平均每日捕获恶意文件5.87件；审计次数最多的是3月12日，达19次；波动最大的是3月4日，较3月3日减少100%；在3月22日至3月24日出现连续3日以上的持续增长。在3月19日至3月21日出现连续3日以上的持续减少。
- 按资产组分布，发生文件安全最多的是内网IP范围，共176次，占总数的96.7%；其次是校内学院虚拟化机器（6次，3.3%）等。

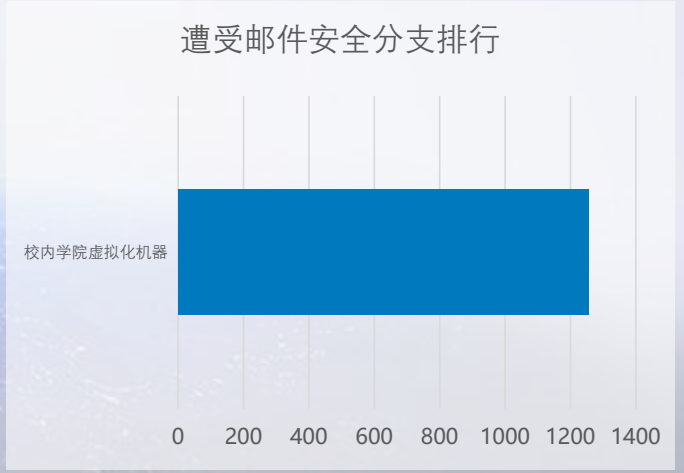




网络安全风险详情-邮件安全

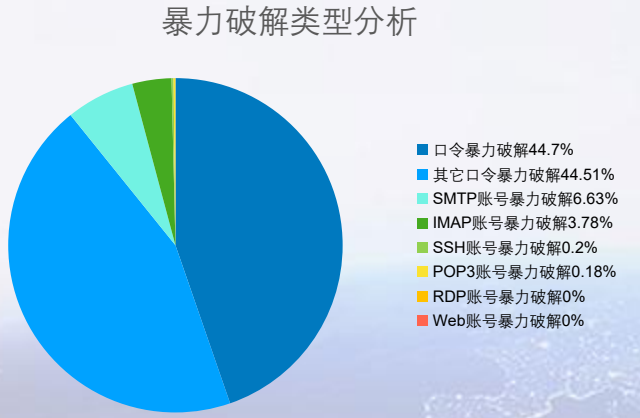
- 邮件是恶意软件分发和网络钓鱼的头号媒介；2026年03月，共捕获钓鱼邮件68.97%867次；垃圾邮件31.03%390次；
- 趋势上，平均每日捕获邮件安全风险40.55件；捕捉最高的是3月29日，达331次；波动最大的是3月29日，较3月28日增加845.71%；在3月3日至3月6日、3月7日至3月9日等出现连续3日以上的持续增长。在3月1日至3月3日、3月12日至3月15日等出现连续3日以上的持续减少。
- 按资产组分布，发生邮件安全最多的是校内学院虚拟化机器，共1257次，占总数的100%；





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03月共捕获暴力破解攻击告警1.94百万次，其中口令暴力破解排名第一，占比44.7%;其次是其它口令暴力破解、SMTP账号暴力破解。
- 暴破频率最高达901次/分钟，该告警于2026年03月07日02时47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

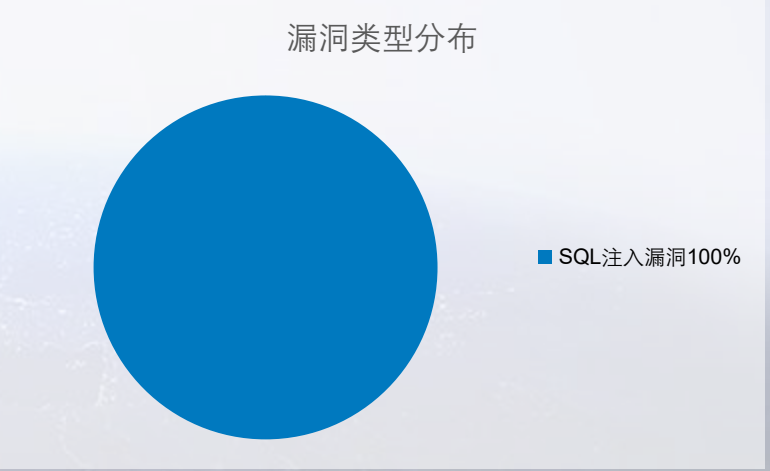


捕获时间：	2026-03-07 02:47:24
攻击者：	118.202.165.10（-）
攻击手段：	账号暴力破解
暴破频率：	最高达901次/分钟
受害者：	校内学院虚拟化机器（202.199.162.124）

网络安全风险详情-业务脆弱性

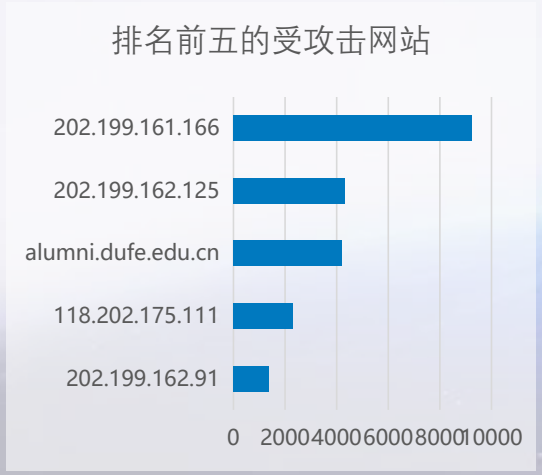
- 业务脆弱性是指“资产中能被威胁所利用的弱点”，包括技术层面的脆弱性，如：漏洞、WEB明文传输、配置错误，还有管理层面的风险，如：弱密码。2026年03月共捕获漏洞1个，Web明文传输163个，配置错误风险378个，弱密码账号119个；
- 捕获最多的是SQL注入漏洞，共捕获1次，占所有漏洞的100%；
- 平均每日捕获高危漏洞0个；捕获次数最多的是0月0日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；

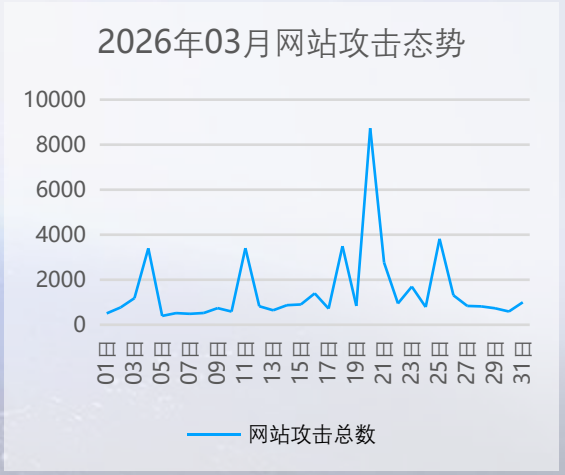
1个	163个	378个	119个
漏洞	Web明文传输	配置风险	弱密码



网络安全风险详情-网站攻击

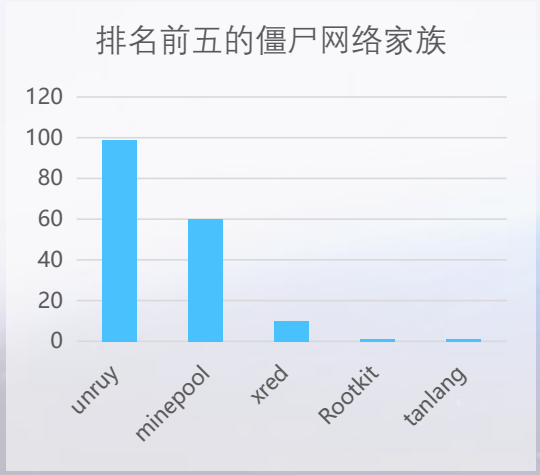
- 2026年03月，共捕获网站类攻击4.62万次，其中被攻击最多的网站是202.199.161.166，达到9244次，占总体的20%；其次是202.199.162.125、alumni.dufe.edu.cn。
- 2026年03月捕获的网站攻击中，既有来自境内的，也有来自境外的；境外攻击源主要来自美国、德国、新加坡、加拿大、立陶宛，这5个国家/地区的网站攻击占总体境外网站攻击的59.32%；境内主要来源辽宁、四川、香港、北京、广东，这5个省份的网站攻击占总体境内网站攻击87.22%，占所有网站攻击的47.79%；
- 趋势上，平均每日捕获网络攻击1491.26次；捕获次数最高的是3月20日，达8733次；波动最大的是3月20日，较3月19日增加944.62%；在3月1日至3月4日、3月7日至3月9日等出现连续3日以上的持续增长。在3月11日至3月13日、3月20日至3月22日等出现连续3日以上的持续减少。

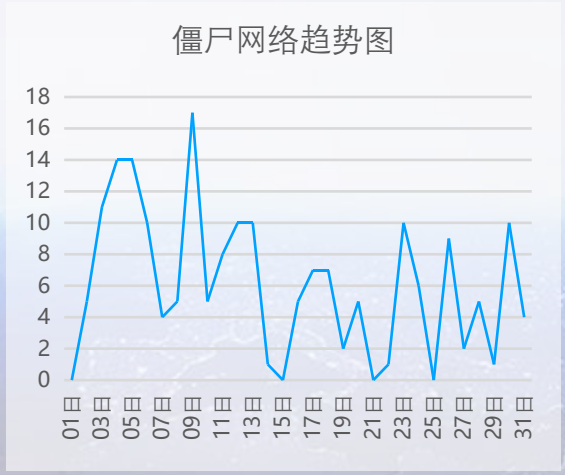


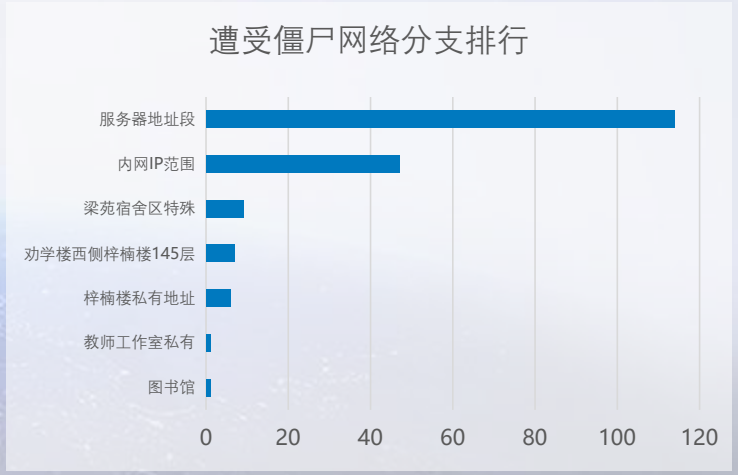


网络安全风险详情-僵尸网络

- 2026年03月，共捕获僵尸网络188次；其中unruy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52.66%；排名第二第三的minepool、xred比例分别为31.91%、5.32%
- 趋势上，平均每日捕获僵尸网络攻击6.06次；捕获次数最高的是3月9日，达17次；波动最大的是3月23日，较3月22日增加900%；在3月1日至3月4日、3月7日至3月9日等出现连续3日以上的持续增长。在3月5日至3月7日、3月13日至3月15日等出现连续3日以上的持续减少。
- 按资产组分布，发生僵尸网络最多的是服务器地址段，共114次，占总数的60.64%；其次是内网IP范围（47次，25%）、梁苑宿舍区特殊（9次，4.79%）等。

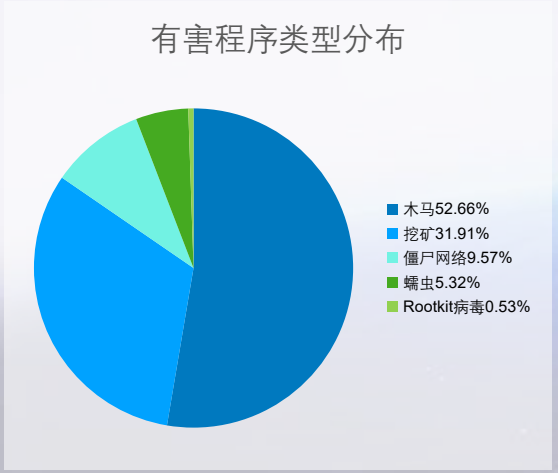


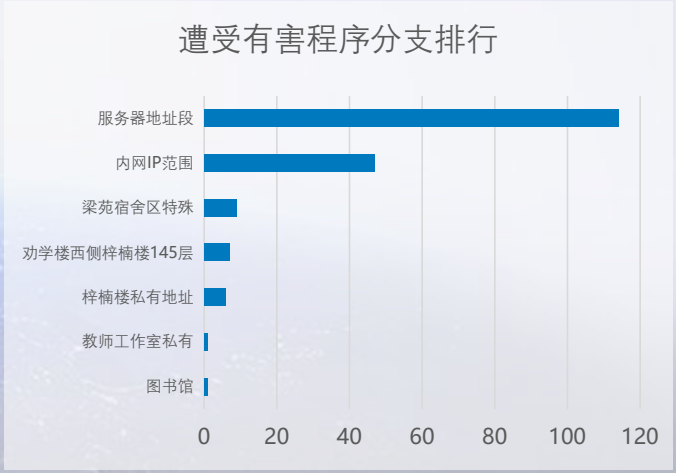




网络安全风险详情-有害程序

- 2026年03月，共捕获有害程序告警188次；其中最为活跃的是木马，共捕获99次，占所有恶意程序捕获数量的52.66%；而排名第二第三的挖矿、僵尸网络的比例分别为31.91%、9.57%
- 趋势上，平均每日捕获有害程序风险6.06次；捕获次数最高的是3月9日，达17次；波动最大的是3月23日，较3月22日增加900%；在3月1日至3月4日、3月7日至3月9日等出现连续3日以上的持续增长。在3月5日至3月7日、3月13日至3月15日等出现连续3日以上的持续减少。
- 按资产组分布，发生有害程序最多的是服务器地址段，共114次，占总数的60.64%；其次是内网IP范围（47次，25%）、梁苑宿舍区特殊（9次，4.79%）等。





东北财经大学
DONGBEI UNIVERSITY OF FINANCE & ECONOMICS

THANK YOU

2026年03月