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04月

目录 CONTENTS

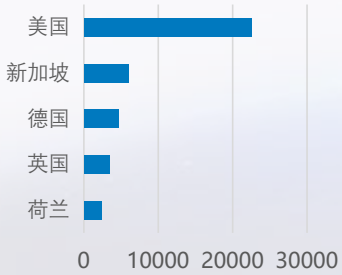
01 内部网络安全情况 - 网络安全整体解读

网络安全整体解读-安全总览

- 共捕获攻击次数1.18千万次,较上个月增加215.88%；平均每日捕获攻击近39.42万次，攻击者数量达1.19万个，来源国家或地区166个，境外主要来自美国、新加坡、德国，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120次；网络攻击事件38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25个；

1.18千万次	1.19万个	132个	120个	38个	36个	1个	25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

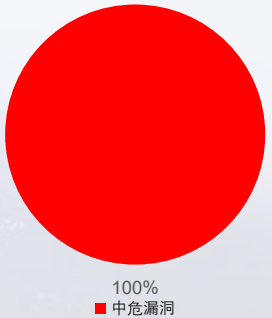
境外攻击源地区



境内攻击源地区

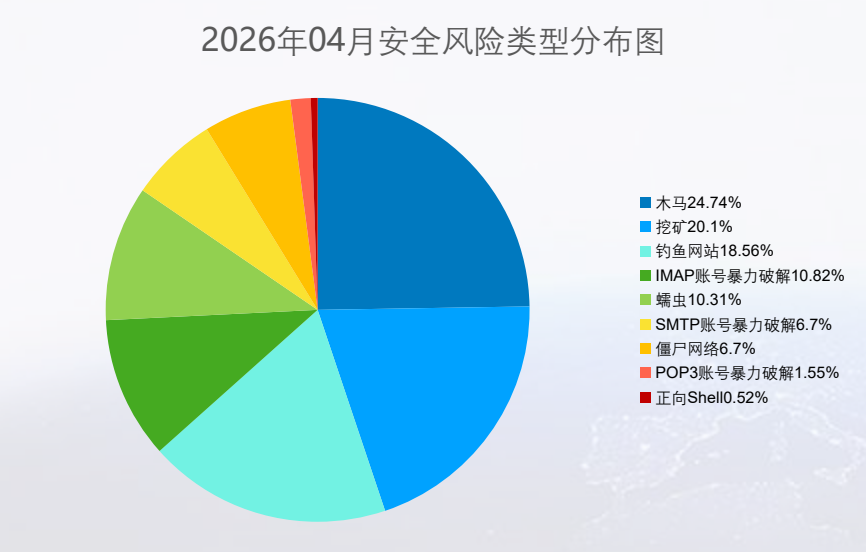
安全风险类型分布

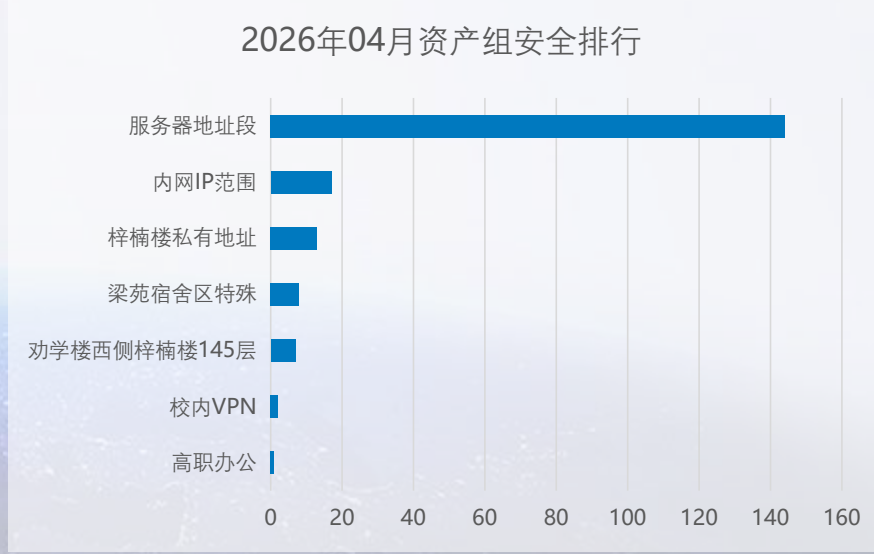
漏洞分布图



网络安全整体解读-安全总览

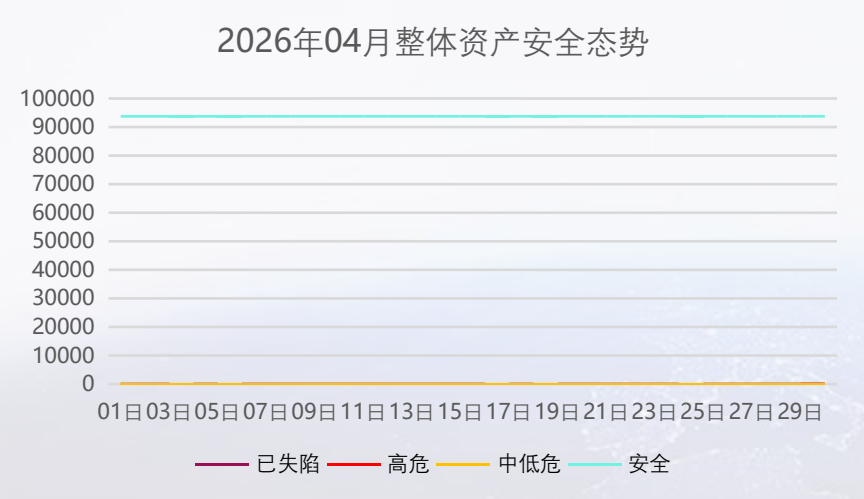
- 2026年04月最突出的安全风险前三名分别是木马、挖矿、钓鱼网站，本月处理这三类风险分别为24.74%、20.1%、18.56%，占本月总风险63.4%；针对这些风险，共处置主机47个/次，处置漏洞0个；
- 按资产组分布，发生安全风险次数最多的是服务器地址段，共144次，占总数的74.23%；其次是内网IP范围（17次，8.76%）、梓楠楼私有地址（13次，6.7%）；安全风险次数最少的是劝学楼西侧梓楠楼145层、校内VPN、高职办公。





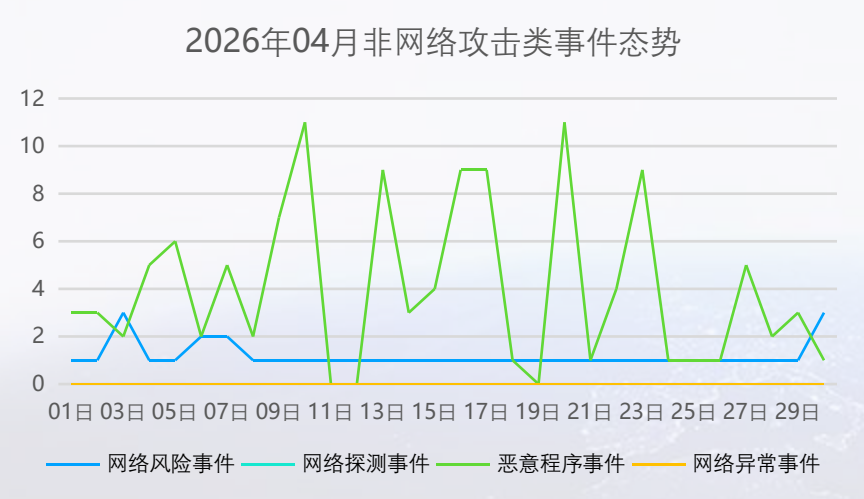
网络安全整体解读-安全态势

- 2026年04月平均每日捕获风险资产4.03个左右，占总资产数（服务器209个、终端92916个）0%；风险资产总数在4月20日达到高峰，共8个，占资产总数0.01%；“已失陷”资产在4月13日增幅最大，增幅达200%，从1个增加到3个；“已失陷”资产数在4月11日经过处置后，同比减少71.43%；“安全”类资产在4月10日至4月12日出现连续3日以上的持续增长；“安全”类资产在4月8日至4月10日、4月12日至4月15日等出现连续3日以上的持续减少；
- 2026年04月共捕获外部网络攻击1.18千万次，平均每日39.42万次；较上个月增加215.88%；在4月15日达到最高的64.15万次；波动最大的是4月2日，较4月1日减少59.73%；在4月6日至4月8日、4月9日至4月15日出现连续3日以上的持续增长。在4月3日至4月6日、4月17日至4月21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

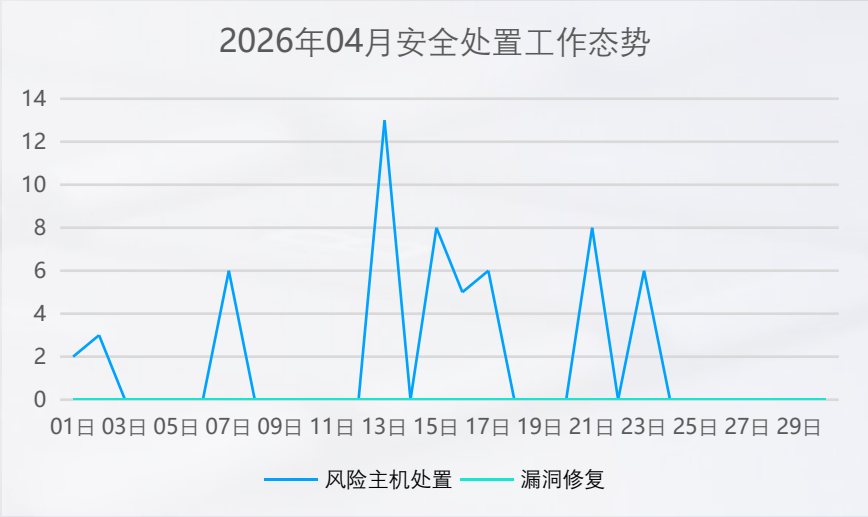
- 2026年04月共捕获有害程序、信息破坏、信息内容安全等其他非网络攻击类事件194次，日均6.47次，其中4月10日最高12次；
- 2026年04月共捕获漏洞1个，平均每日0.03个；捕获次数最高的是4月14日，达1个；按日同比，在4月15日经过加固后；同比减少100%；
- 其中高危漏洞0个，占比0%，平均每日0个；高危漏洞捕获次数最高的是0月0日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；



网络安全整体解读-安全处置工作概览

- 2026年04月共处置风险主机57个，较上个月减少33.72%；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	1.18千万次
修复漏洞	0次
处置主机	57条
合规检查	0次
重大活动保障	0次

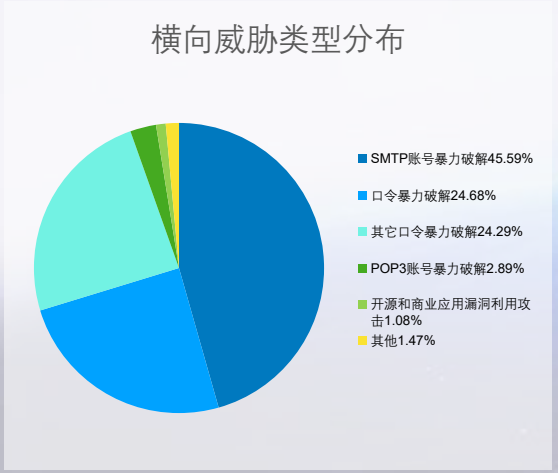


01 内部网络安全情况 - 网络安全风险详情

—— 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

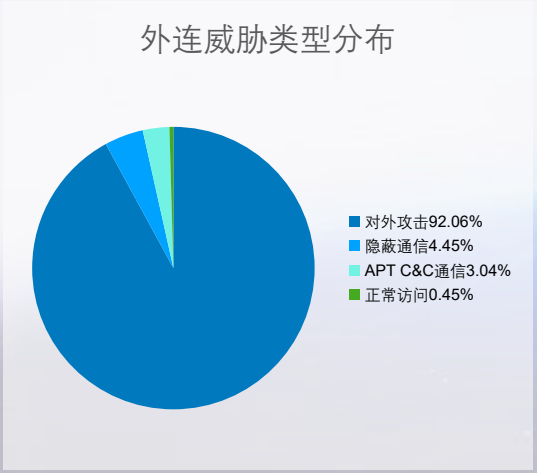
网络安全风险详情-横向威胁

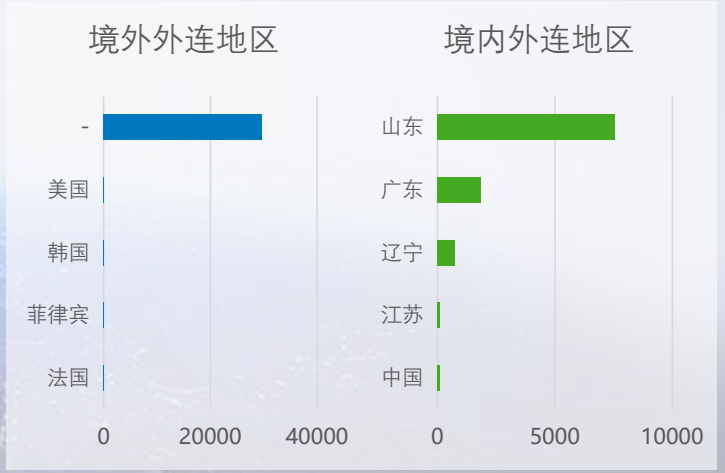
- 在2026年04月共捕获横向威胁主机688台，横向威胁事件93.58万件，其中SMTP账号暴力破解排名第一，占比45.59%；其次是口令暴力破解、其它口令暴力破解。
- 趋势上，平均每日发起横向威胁3.12万件；捕获次数最多的是4月29日，达4.67万次；波动最大的是4月3日，较4月2日减少35.33%；在4月3日至4月6日、4月15日至4月19日等出现连续3日以上的持续增长。在4月1日至4月3日、4月6日至4月9日等出现连续3日以上的持续减少。
- 按资产组分布，发生横向威胁最多的是校内学院虚拟化机器，共82.68万次，占总数的88.36%；其次是锐捷交换机（6.55万次，7%）、内网IP范围（3.85万次，4.11%）等。



网络安全风险详情-外连威胁

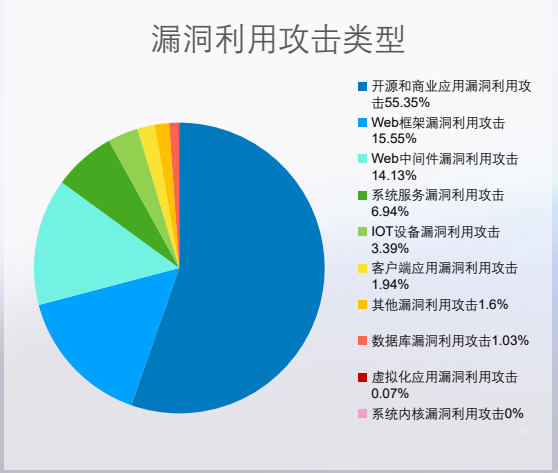
- 在2026年04月共捕获外连威胁主机703台，外连威胁事件4.06万件，其中对外攻击排名第一，占比92.06%；其次是隐蔽通信、APT C&C通信。
- 趋势上，平均每日发起外连威胁1351.73件；捕获次数最多的是4月29日，达7021次；波动最大的是4月30日，较4月29日减少84.35%；在4月8日至4月10日、4月15日至4月17日等出现连续3日以上的持续增长。在4月12日至4月15日、4月17日至4月19日等出现连续3日以上的持续减少。
- 风险主机外连地区既有境内也有境外；境外外连地区主要来自-、美国、韩国、菲律宾、法国，这5个国家/地区的外连次数占总体境外外连地区的99.93%；境内主要来源山东、广东、辽宁、江苏、中国，这5个省份的外连次数占总体外连次数95.72%，占总外连次数的25.45%；

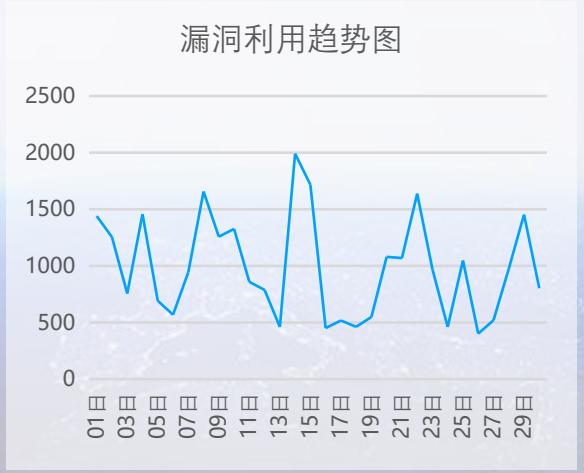




网络安全风险详情-漏洞利用

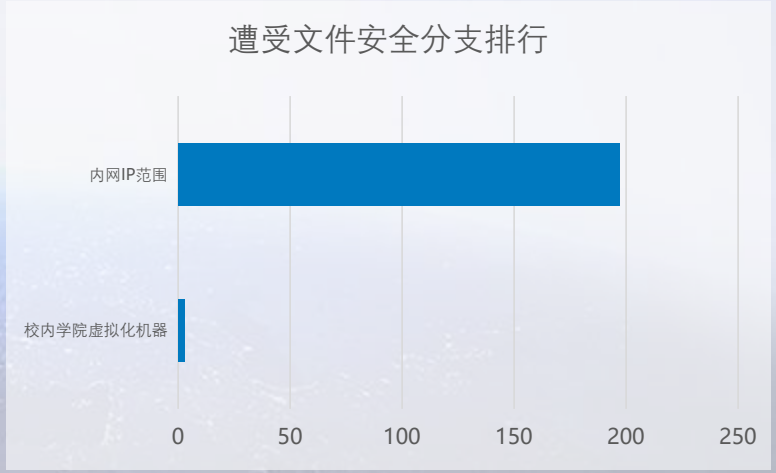
- 漏洞利用是最常见的一种网络攻击，2026年04月共捕获漏洞利用攻击告警2.96万次，其中开源和商业应用漏洞利用攻击排名第一，占比55.35%；其次是Web框架漏洞利用攻击、Web中间件漏洞利用攻击。
- 趋势上，平均每日发起漏洞利用攻击985.6件；捕获次数最多的是4月14日，达1991次；波动最大的是4月14日，较4月13日增加331.89%；在4月6日至4月8日、4月18日至4月20日等出现连续3日以上的持续增长。在4月1日至4月3日、4月4日至4月6日等出现连续3日以上的持续减少。
- 按资产组分布，发生漏洞利用攻击最多的是服务器地址段，共1.38万次，占总数的54.13%；其次是校内学院虚拟化机器（7183次，28.1%）、内网IP范围（3324次，13.01%）等。





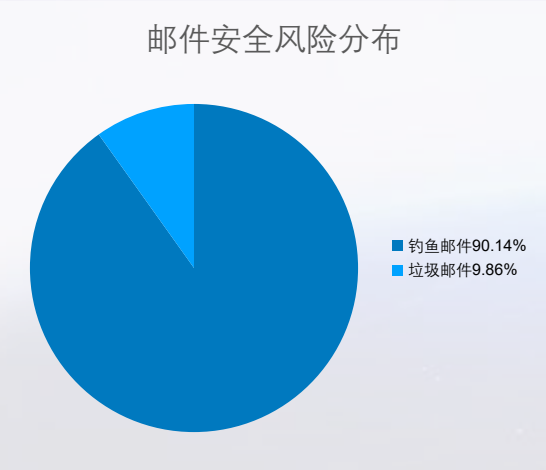
网络安全风险详情-文件安全

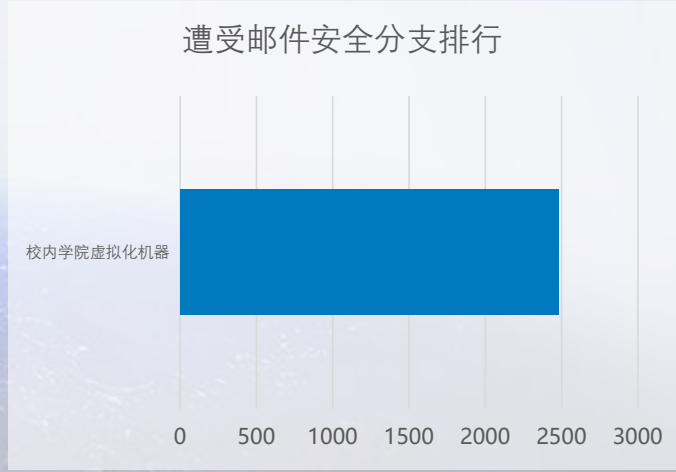
- 文件是病毒传播的常见手段；2026年04月共查杀文件796872余次，确认为恶意文件的有200个；
- 趋势上，平均每日捕获恶意文件6.67件；审计次数最多的是4月2日，达18次；波动最大的是4月3日，较4月2日减少100%；
- 按资产组分布，发生文件安全最多的是内网IP范围，共197次，占总数的98.5%；其次是校内学院虚拟化机器（3次，1.5%）等。



网络安全风险详情-邮件安全

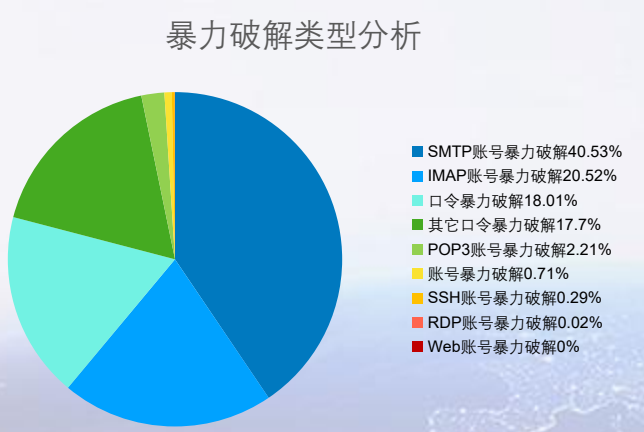
- 邮件是恶意软件分发和网络钓鱼的头号媒介；2026年04月，共捕获钓鱼邮件90.14%2239次；垃圾邮件9.86%245次；
- 趋势上，平均每日捕获邮件安全风险82.8件；捕捉最高的是4月19日，达464次；波动最大的是4月13日，较4月12日减少94.1%；在4月8日至4月10日、4月13日至4月16日等出现连续3日以上的持续增长。在4月1日至4月4日出现连续3日以上的持续减少。
- 按资产组分布，发生邮件安全最多的是校内学院虚拟化机器，共2484次，占总数的100%；





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04月共捕获暴力破解攻击告警31.92万次，其中SMTP账号暴力破解排名第一，占比40.53%;其次是IMAP账号暴力破解、口令暴力破解。
- 暴破频率最高达901次/分钟，该告警于2026年04月02日01时36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

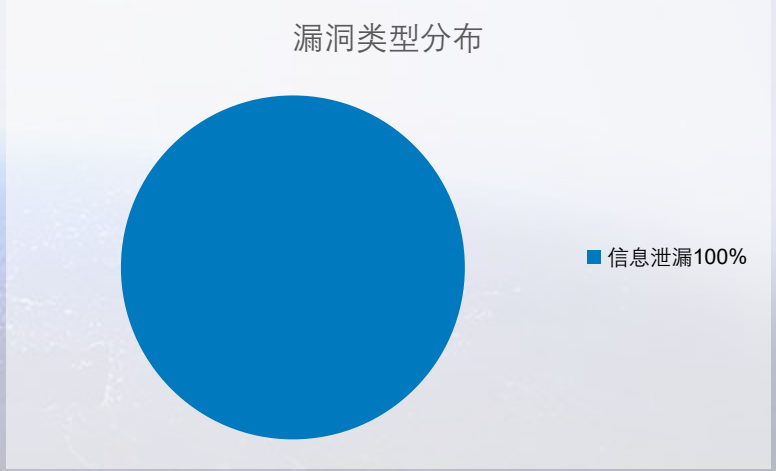


捕获时间：	2026-04-02 01:36:40
攻击者：	118.202.165.12（-）
攻击手段：	账号暴力破解
暴破频率：	最高达901次/分钟
受害者：	校内学院虚拟化机器（202.199.162.124）

网络安全风险详情-业务脆弱性

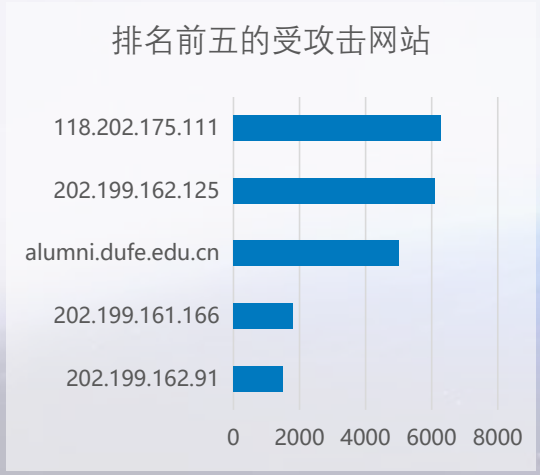
- 业务脆弱性是指“资产中能被威胁所利用的弱点”，包括技术层面的脆弱性，如：漏洞、WEB明文传输、配置错误，还有管理层面的风险，如：弱密码。2026年04月共捕获漏洞1个，Web明文传输146个，配置错误风险366个，弱密码账号83个；
- 捕获最多的是信息泄漏，共捕获1次，占所有漏洞的100%；
- 平均每日捕获高危漏洞0个；捕获次数最多的是0月0日，达0个；按日同比未出现20%以上的波动，总体趋势比较平稳；

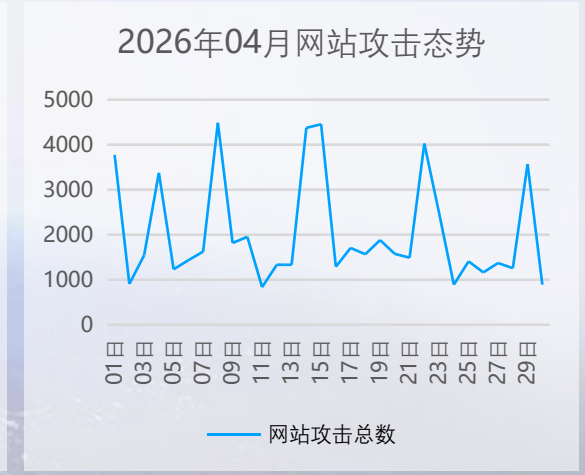
1个	146个	366个	83个
漏洞	Web明文传输	配置风险	弱密码



网络安全风险详情-网站攻击

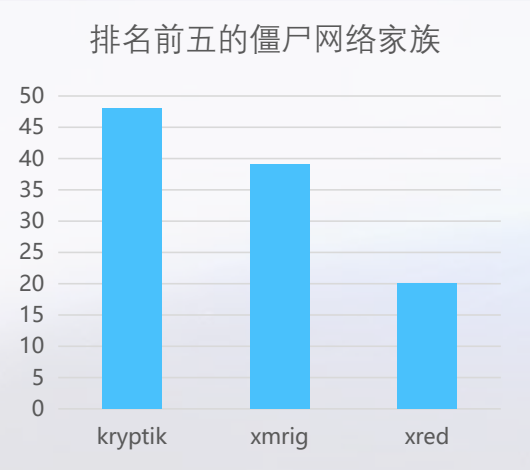
- 2026年04月，共捕获网站类攻击6.1万次，其中被攻击最多的网站是118.202.175.111，达到6276次，占总体的10.28%；其次是202.199.162.125、alumni.dufe.edu.cn。
- 2026年04月捕获的网站攻击中，既有来自境内的，也有来自境外的；境外攻击源主要来自美国、德国、新加坡、荷兰、英国，这5个国家/地区的网站攻击占总体境外网站攻击的58.25%；境内主要来源辽宁、香港、北京、广西、河南，这5个省份的网站攻击占总体境内网站攻击84.48%，占所有网站攻击的37.4%；
- 趋势上，平均每日捕获网络攻击2034.87次；捕获次数最高的是4月8日，达4486次；波动最大的是4月14日，较4月13日增加228.38%；在4月2日至4月4日、4月5日至4月8日等出现连续3日以上的持续增长。在4月19日至4月21日、4月22日至4月24日出现连续3日以上的持续减少。

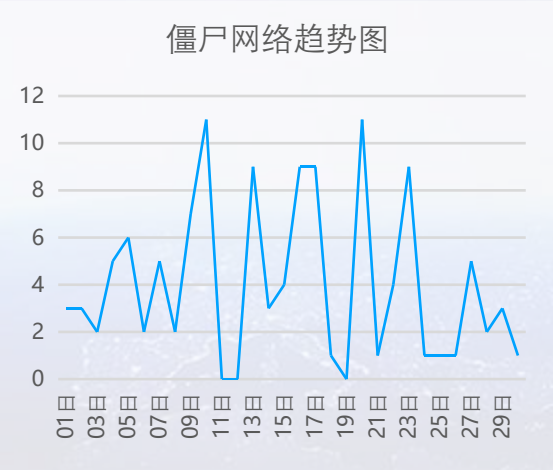


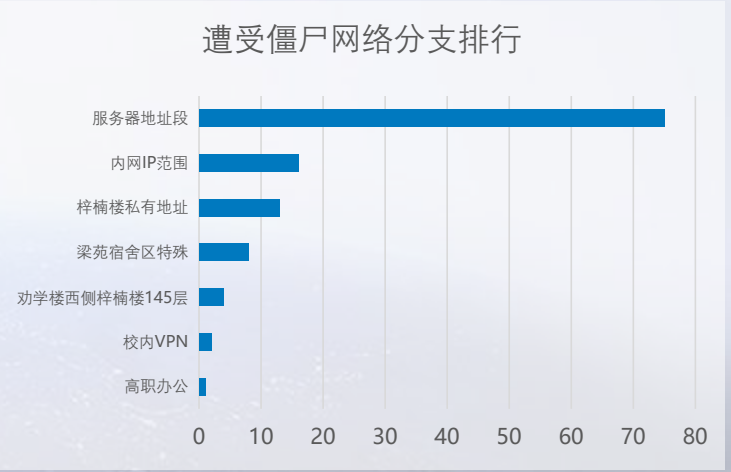


网络安全风险详情-僵尸网络

- 2026年04月，共捕获僵尸网络120次；其中kryptik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40%；排名第二第三的xmrig、xred比例分别为32.5%、16.67%
- 趋势上，平均每日捕获僵尸网络攻击4次；捕获次数最高的是4月10日，达11次；波动最大的是4月11日，较4月10日减少100%；在4月3日至4月5日、4月8日至4月10日等出现连续3日以上的持续增长。在4月17日至4月19日出现连续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75次，占总数的62.5%；其次是内网IP范围（16次，13.33%）、梓楠楼私有地址（13次，10.83%）等。

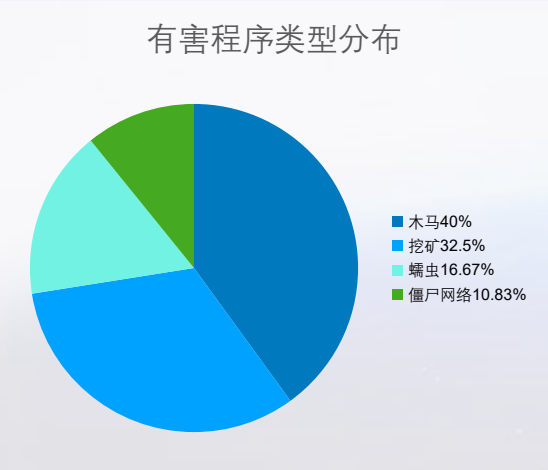


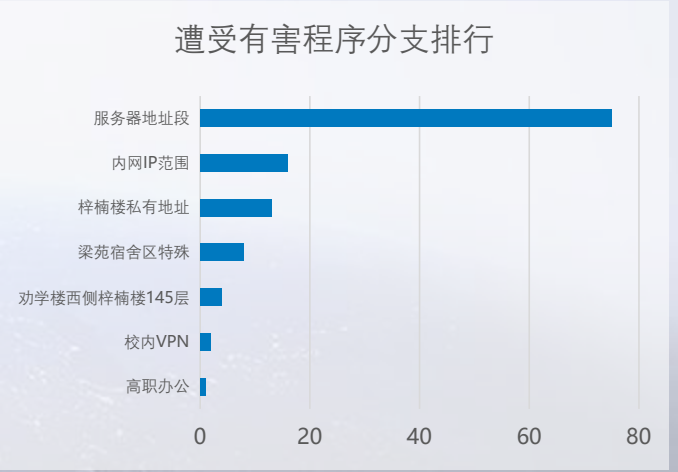




网络安全风险详情-有害程序

- 2026年04月，共捕获有害程序告警120次；其中最为活跃的是木马，共捕获48次，占所有恶意程序捕获数量的40%；而排名第二第三的挖矿、蠕虫的比例分别为32.5%、16.67%
- 趋势上，平均每日捕获有害程序风险4次；捕获次数最高的是4月10日，达11次；波动最大的是4月11日，较4月10日减少100%；在4月3日至4月5日、4月8日至4月10日等出现连续3日以上的持续增长。在4月17日至4月19日出现连续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75次，占总数的62.5%；其次是内网IP范围（16次，13.33%）、梓楠楼私有地址（13次，10.83%）等。





THANK YOU

2026年04月