



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05月

## 01 内部网络安全情况

### 1.1 网络安全整体解读

- ◆ 安全总览
- ◆ 安全态势
- ◆ 安全处置工作概览

### 1.2 网络安全风险详情

- |        |         |
|--------|---------|
| ◆ 横向威胁 | ◆ 暴力破解  |
| ◆ 外连威胁 | ◆ 业务脆弱性 |
| ◆ 漏洞利用 | ◆ 网站攻击  |
| ◆ 文件安全 | ◆ 僵尸网络  |
| ◆ 邮件安全 | ◆ 有害程序  |



## 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1.89百万次,较上个月增加16.13%; 平均每日捕获攻击近6.11万次, 攻击者数量达2.94万个, 来源国家或地区114个, 境外主要来自新加坡、美国、荷兰, 境内主要是河北、北京、浙江。外部攻击形势依旧严峻;
- 共捕获恶意程序事件930次; 网络攻击事件63次; 未发生网络探测事件、网络异常事件;
- 共捕获漏洞3个; 弱密码13个;

1.89百万次 ↑

攻击总数

2.94万个 ↑

攻击者

82个 ↑

境外攻击地区

930个 ↑

恶意程序事件

63个 ↑

网络攻击事件

6个 ↓

其他

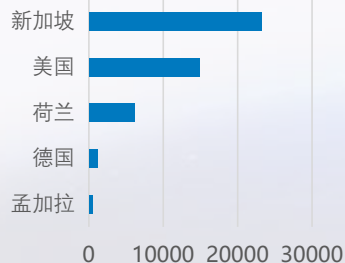
3个 ↑

漏洞总数

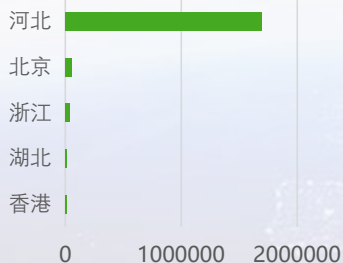
13个 ↑

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

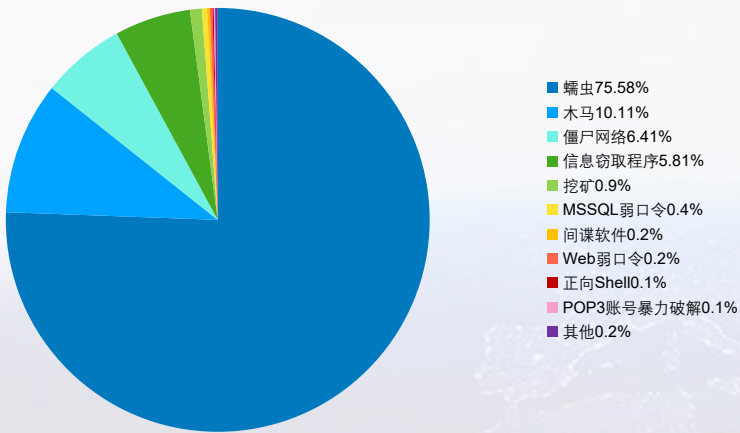




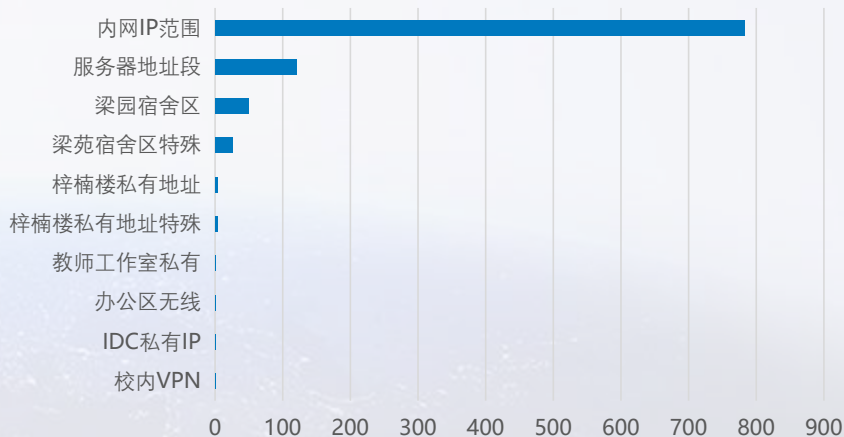
## 网络安全整体解读-安全总览

- 2025年05月最突出的安全风险前三名分别是蠕虫、木马、僵尸网络，本月处理这三类风险分别为75.58%、10.11%、6.41%，占本月总风险92.09%；针对这些风险，共处置主机630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782次，占总数的78.28%；其次是服务器地址段（121次，12.11%）、梁园宿舍区（49次，4.9%）；安全风险次数最少的是办公区无线、IDC私有IP、校内VPN。

2025年05月安全风险类型分布图



2025年05月资产组安全排行

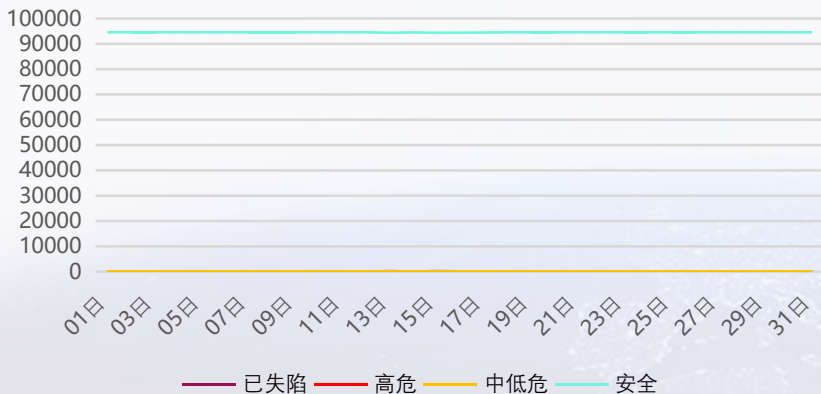




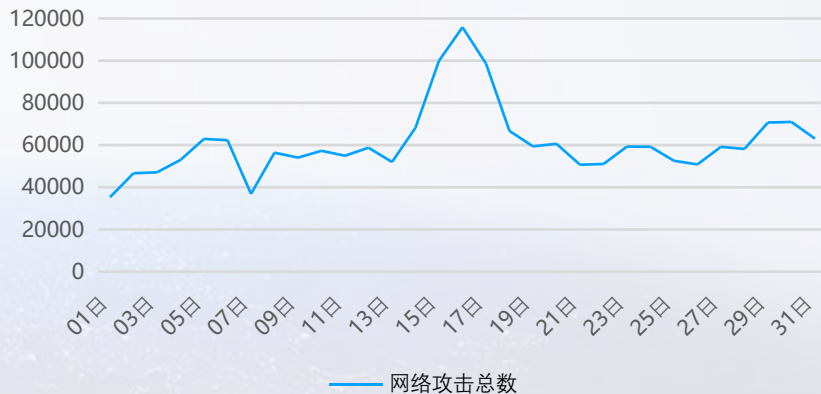
## 网络安全整体解读-安全态势

- 2025年05月平均每日捕获风险资产29.52个左右，占总资产数（服务器225个、终端93697个）0.03%；风险资产总数在5月13日达到高峰，共194个，占资产总数0.21%；“已失陷”资产在5月13日增幅最大，增幅达2055.56%，从9个增加到194个；“已失陷”资产数在5月18日经过处置后，同比减少89.66%；“高危”资产数在5月7日经过处置后，同比减少100%；“安全”类资产在5月15日至5月19日、5月21日至5月23日出现连续3日以上的持续增长；“安全”类资产在5月29日至5月31日出现连续3日以上的持续减少；
- 2025年05月共捕获外部网络攻击1.89百万次，平均每日6.11万次；较上个月增加16.13%；在5月16日达到最高的11.59万次；波动最大的是5月7日，较5月6日减少40.8%；在5月1日至5月5日、5月13日至5月16日等出现连续3日以上的持续增长。在5月5日至5月7日、5月16日至5月19日等出现连续3日以上的持续减少。

2025年05月整体资产安全态势



2025年05月网络攻击态势





## 网络安全整体解读-安全态势

- 2025年05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999次，日均32.23次，其中5月13日最高196次；
- 2025年05月共捕获漏洞3个，平均每日0.1个；捕获次数最高的是5月8日，达3个；按日同比，在5月9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；

2025年05月非网络攻击类事件态势



2025年05月漏洞态势



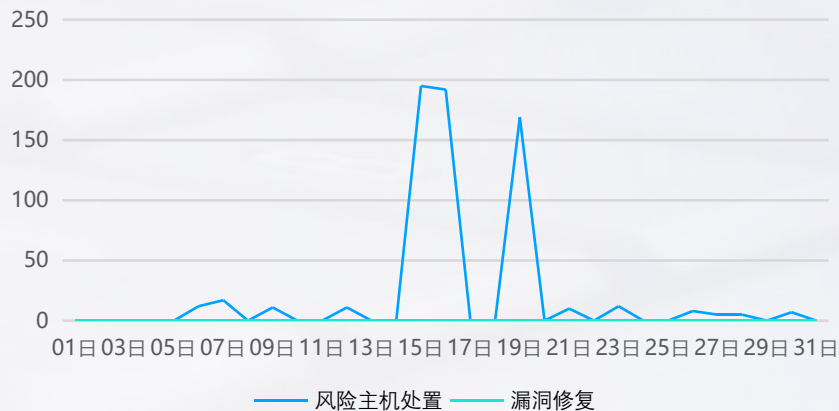


## 网络安全整体解读-安全处置工作概览

- 2025年05月共处置风险主机654个，较上个月增加65.57%；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。



2025年05月安全处置工作态势







## 01 内部网络安全情况 - 网络安全风险详情

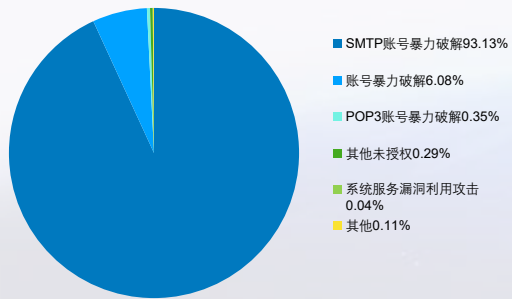
—— 本章节将详细阐述暴力破解、网站攻击、邮件安全、僵尸网络、恶意程序、业务脆弱性的捕获统计和趋势分析



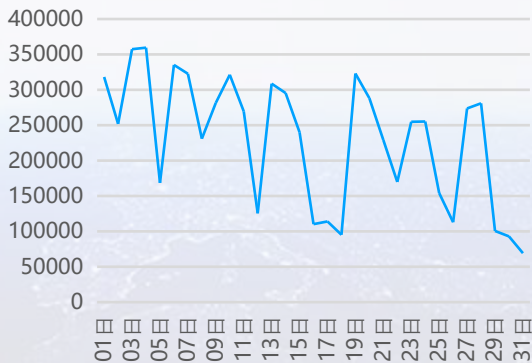
## 网络安全风险详情-横向威胁

- 在2025年05月共捕获横向威胁主机633台，横向威胁事件7.11百万件，其中SMTP账号暴力破解排名第一，占比93.13%；其次是账号暴力破解、POP3账号暴力破解。
- 趋势上，平均每日发起横向威胁22.94万件；捕获次数最多的是5月4日，达35.95万次；波动最大的是5月19日，较5月18日增加239.39%；在5月2日至5月4日、5月8日至5月10日等出现连续3日以上的持续增长。在5月6日至5月8日、5月10日至5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6.76百万次，占总数的95.04%；其次是锐捷交换机（23.59万次，3.32%）、内网IP范围（9.15万次，1.29%）等。

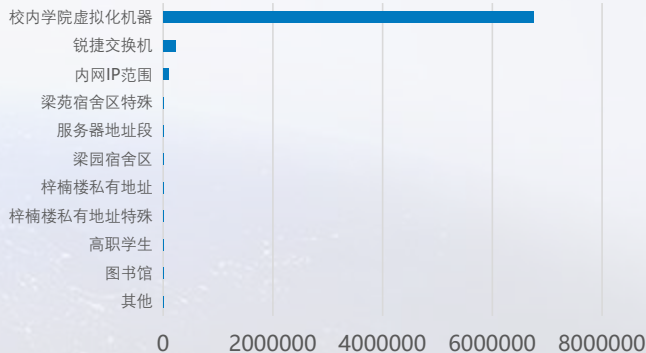
横向威胁类型分布



横向威胁趋势图



遭受横向威胁分支排行

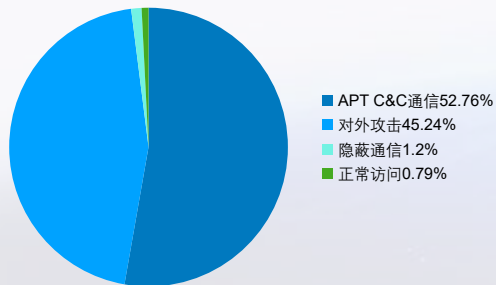




## 网络安全风险详情-外连威胁

- 在2025年05月共捕获外连威胁主机359台，外连威胁事件6.26万件，其中APT C&C通信排名第一，占比52.76%；其次是对外攻击、隐蔽通信。
- 趋势上，平均每日发起外连威胁2018.48件；捕获次数最多的是5月15日，达6859次；波动最大的是5月15日，较5月14日增加150.42%；在5月1日至5月5日、5月8日至5月10日出现连续3日以上的持续增长。在5月10日至5月12日、5月15日至5月18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、荷兰、日本，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、河北，这5个省份的外连次数占总体外连次数77.42%，占总外连次数的2.8%；

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

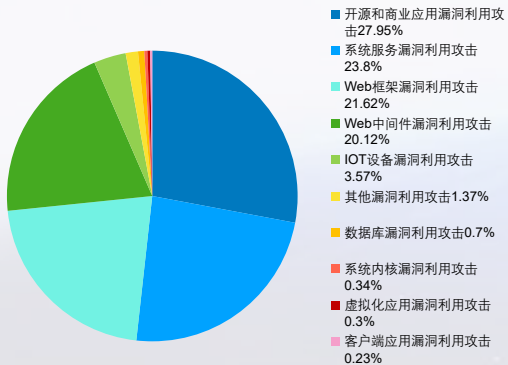




## 网络安全风险详情-漏洞利用

- 漏洞利用是最常见的一种网络攻击，2025年05月共捕获漏洞利用攻击告警7894次，其中开源和商业应用漏洞利用攻击排名第一，占比27.95%；其次是系统服务漏洞利用攻击、Web框架漏洞利用攻击。
- 趋势上，平均每日发起漏洞利用攻击254.65件；捕获次数最多的是5月14日，达1554次；波动最大的是5月15日，较5月14日减少83.27%；在5月4日至5月6日、5月10日至5月12日等出现连续3日以上的持续增长。在5月6日至5月8日、5月14日至5月17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2880次，占总数的38.88%；其次是校内学院虚拟化机器（2572次，34.72%）、内网IP范围（1546次，20.87%）等。

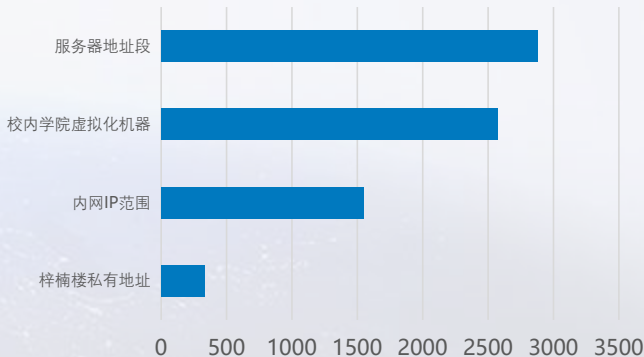
漏洞利用攻击类型



漏洞利用趋势图



遭受漏洞利用攻击分支排行

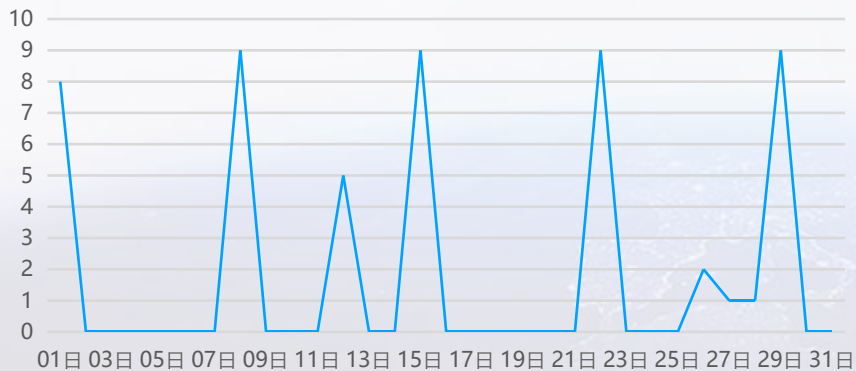




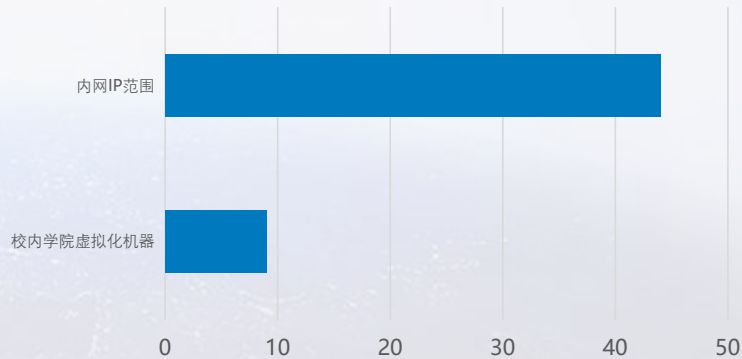
## 网络安全风险详情-文件安全

- 文件是病毒传播的常见手段；2025年05月共查杀文件984777余次，确认为恶意文件的有53个；
- 趋势上，平均每日捕获恶意文件1.71件；审计次数最多的是5月8日，达9次；波动最大的是5月2日，较5月1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44次，占总数的83.02%；其次是校内学院虚拟化机器（9次，16.98%）等。

文件威胁趋势图



遭受文件安全分支排行

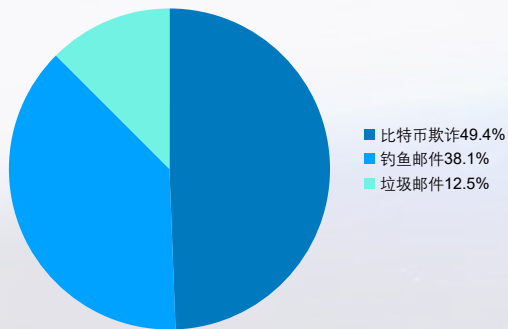




## 网络安全风险详情-邮件安全

- 邮件是恶意软件分发和网络钓鱼的头号媒介；2025年05月，共捕获比特币欺诈49.4%2043次；钓鱼邮件38.1%1576次；垃圾邮件12.5%517次；
- 趋势上，平均每日捕获邮件安全风险133.42件；捕捉最高的是5月30日，达1214次；波动最大的是5月30日，较5月29日增加4958.33%；在5月5日至5月7日、5月11日至5月13日出现连续3日以上的持续增长。在5月7日至5月11日、5月15日至5月18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4136次，占总数的100%；

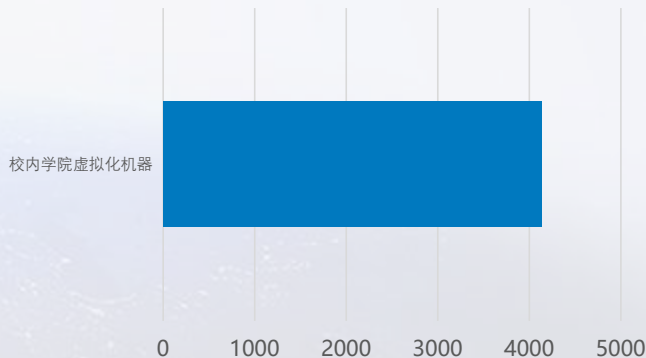
邮件安全风险分布



邮件安全趋势图



遭受邮件安全分支排行

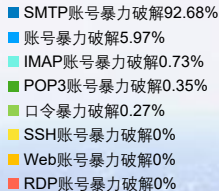




## 网络安全风险详情-暴力破解

- 暴力破解是最常见的一种网络攻击，2025年05月共捕获暴力破解攻击告警5.4百万次，其中SMTP账号暴力破解排名第一，占比92.68%;其次是账号暴力破解、IMAP账号暴力破解。
- 暴破频率最高达901次/分钟，该告警于2025年05月15日10时57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202.199.162.125

暴力破解类型分析



捕获时间: 2025-05-15 10:57:38  
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  
(202.199.162.125)



## 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05月共捕获漏洞3个，Web明文传输186个，配置错误风险145个，弱密码账号27个；
- 捕获最多的是SQL注入漏洞，共捕获3次，占有漏洞的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；

3个

漏洞

186个

Web明文传输

145个

配置风险

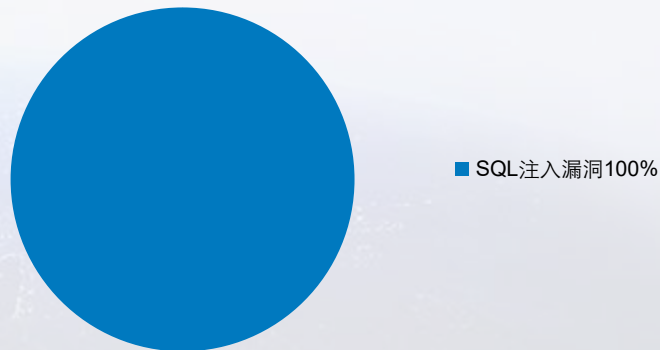
27个

弱密码

2025年05月漏洞态势



漏洞类型分布



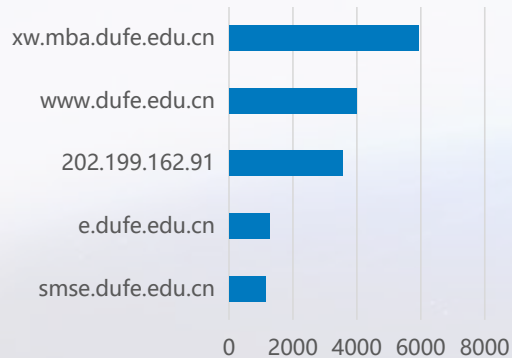




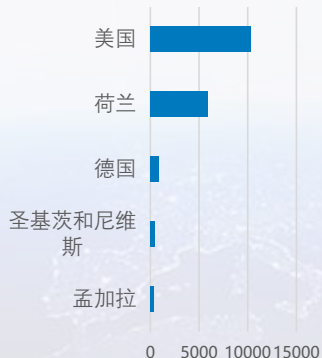
## 网络安全风险详情-网站攻击

- 2025年05月，共捕获网站类攻击5.73万次，其中被攻击最多的网站是xw.mba.dufe.edu.cn，达到5929次，占总体的10.35%；其次是www.dufe.edu.cn、202.199.162.91。
- 2025年05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、德国、圣基茨和尼维斯、孟加拉，这5个国家/地区的网站攻击占总体境外网站攻击的87.97%；境内主要来源浙江、黑龙江、北京、香港、江苏，这5个省份的网站攻击占总体境内网站攻击94.77%，占有网站攻击的61.14%；
- 趋势上，平均每日捕获网络攻击1848.39次；捕获次数最高的是5月5日，达5851次；波动最大的是5月5日，较5月4日增加890.02%；在5月18日至5月20日、5月21日至5月24日等出现连续3日以上的持续增长。在5月2日至5月4日、5月5日至5月7日等出现连续3日以上的持续减少。

排名前五的受攻击网站



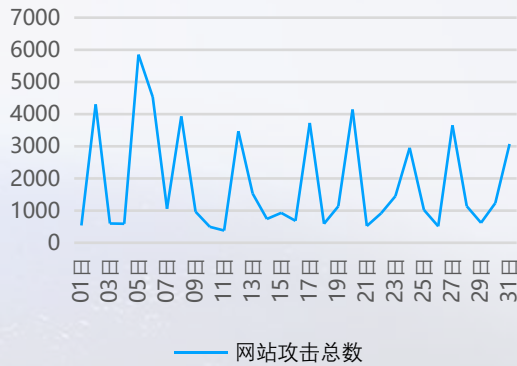
境外攻击源地区



境内攻击源地区



2025年05月网站攻击态势

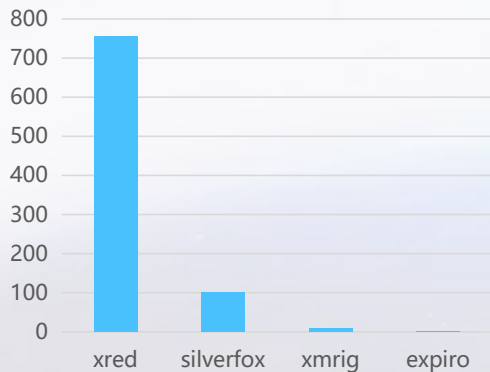




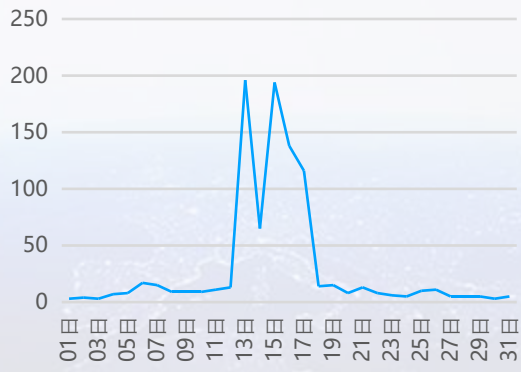
## 网络安全风险详情-僵尸网络

- 2025年05月，共捕获僵尸网络930次；其中xred家族是攻击态势最为活跃的僵尸网络家族，占有僵尸网络拦截数量的81.18%；排名第二第三的silverfox、xmrig比例分别为10.86%、0.97%
- 趋势上，平均每日捕获僵尸网络攻击30次；捕获次数最高的是5月13日，达196次；波动最大的是5月13日，较5月12日增加1407.69%；在5月3日至5月6日、5月10日至5月13日等出现连续3日以上的持续增长。在5月6日至5月8日、5月15日至5月18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754次，占总数的81.08%；其次是服务器地址段（89次，9.57%）、梁园宿舍区（49次，5.27%）等。

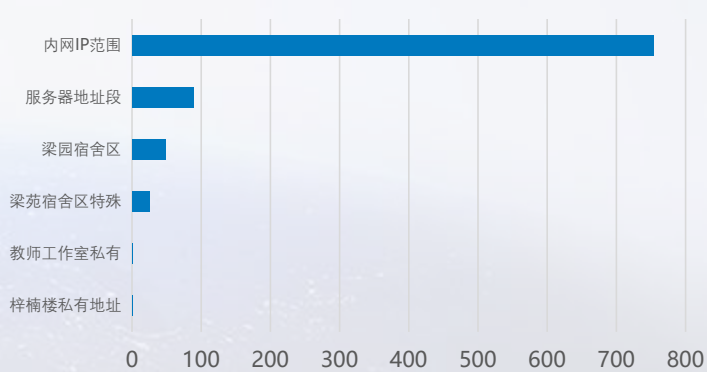
排名前五的僵尸网络家族



僵尸网络趋势图



遭受僵尸网络分支排行

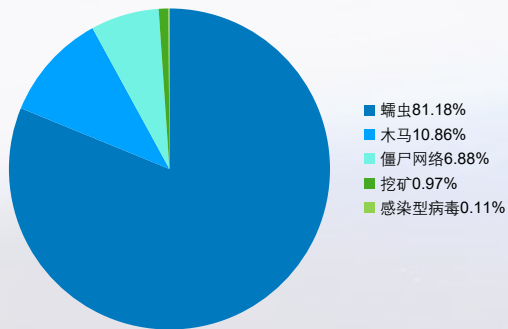




## 网络安全风险详情-有害程序

- 2025年05月，共捕获有害程序告警930次；其中最为活跃的是蠕虫，共捕获755次，占有恶意程序捕获数量的81.18%；而排名第二第三的木马、僵尸网络的比例分别为10.86%、6.88%
- 趋势上，平均每日捕获有害程序风险30次；捕获次数最高的是5月13日，达196次；波动最大的是5月13日，较5月12日增加1407.69%；在5月3日至5月6日、5月10日至5月13日等出现连续3日以上的持续增长。在5月6日至5月8日、5月15日至5月18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754次，占总数的81.08%；其次是服务器地址段（89次，9.57%）、梁园宿舍区（49次，5.27%）等。

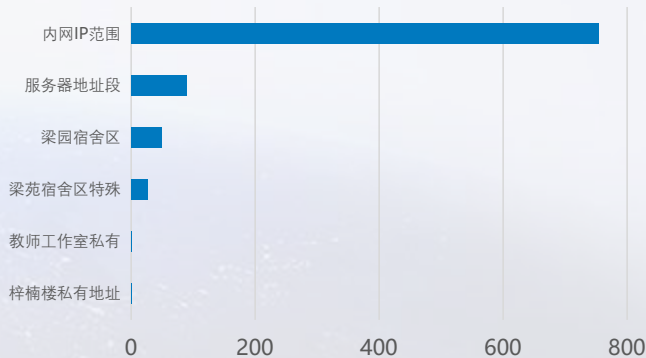
有害程序类型分布



有害程序趋势图



遭受有害程序分支排行





东北财经大学  
DONGBEI UNIVERSITY OF FINANCE & ECONOMICS

# THANK YOU

2025年05月