



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08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2千万次,较上个月减少2.61%; 平均每日捕获攻击近64.61万次, 攻击者数量达10.7万个, 来源国家或地区194个, 境外主要来自美国、新加坡、巴西, 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69次; 网络攻击事件49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11个;

2千万次



攻击总数

10.7万个



攻击者

159个



境外攻击地区

69个



恶意程序事件

49个



网络攻击事件

8个

其他

0个

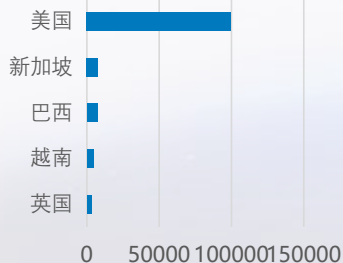
漏洞总数

11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



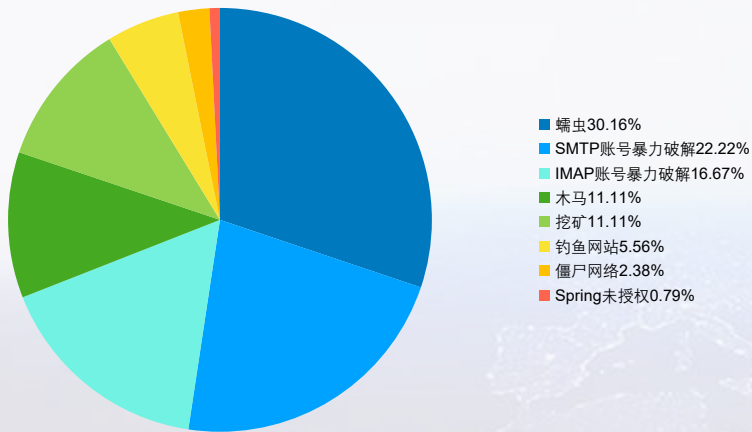
暂无数据



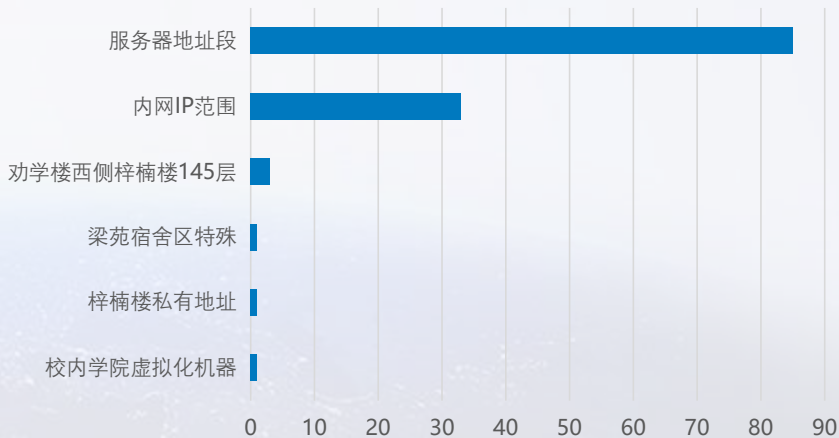
网络安全整体解读-安全总览

- 2026年08月最突出的安全风险前三名分别是蠕虫、SMTP账号暴力破解、IMAP账号暴力破解，本月处理这三类风险分别为30.16%、22.22%、16.67%，占本月总风险69.05%；针对这些风险，共处置主机10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85次，占总数的67.46%；其次是内网IP范围（33次，26.19%）、劝学楼西侧梓楠楼145层（3次，2.38%）；安全风险次数最少的是梁苑宿舍区特殊、梓楠楼私有地址、校内学院虚拟化机器。

2026年08月安全风险类型分布图



2026年08月资产组安全排行





网络安全整体解读-安全态势

- 2026年08月平均每日捕获风险资产2.9个左右，占总资产数（服务器204个、终端82502个）0%；风险资产总数在8月31日达到高峰，共8个，占资产总数0.01%；“已失陷”资产在8月31日增幅最大，增幅达700%，从1个增加到8个；“已失陷”资产数在8月7日经过处置后，同比减少80%；“高危”资产数在8月26日经过处置后，同比减少100%；“安全”类资产在8月3日至8月5日、8月10日至8月12日出现连续3日以上的持续增长；“安全”类资产在8月16日至8月18日出现连续3日以上的持续减少；
- 2026年08月共捕获外部网络攻击2千万次，平均每日64.61万次；较上个月减少2.61%；在8月31日达到最高的79.14万次；波动最大的是8月22日，较8月21日增加53.37%；在8月1日至8月5日、8月10日至8月12日等出现连续3日以上的持续增长。在8月5日至8月7日、8月8日至8月10日等出现连续3日以上的持续减少。

2026年08月整体资产安全态势



2026年08月网络攻击态势

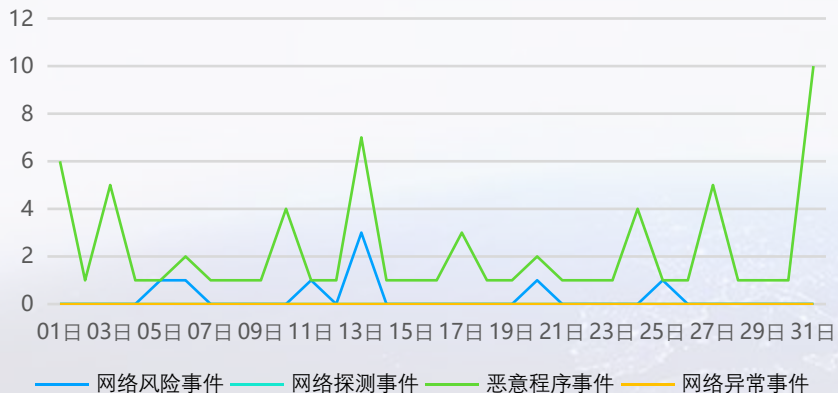




网络安全整体解读-安全态势

- 2026年08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126次，日均4.06次，其中8月13日最高10次；
- 2026年08月共捕获漏洞0个，平均每日0个；捕获次数最高的是8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8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；

2026年08月非网络攻击类事件态势



2026年08月漏洞态势



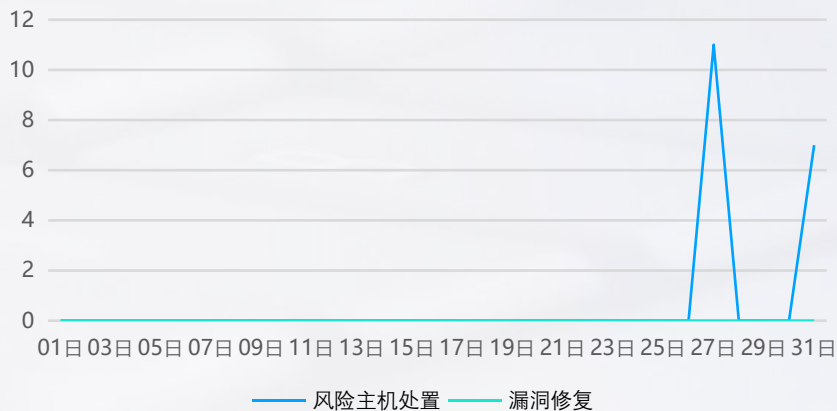


网络安全整体解读-安全处置工作概览

- 2026年08月共处置风险主机18个，较上个月减少82.18%；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。



2026年08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

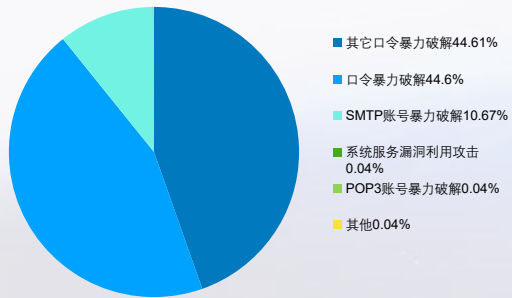
—— 本章节将详细阐述暴力破解、网站攻击、邮件安全、僵尸网络、恶意程序、业务脆弱性的捕获统计和趋势分析



网络安全风险详情-横向威胁

- 在2026年08月共捕获横向威胁主机470台，横向威胁事件5百万件，其中其它口令暴力破解排名第一，占比44.61%；其次是口令暴力破解、SMTP账号暴力破解。
- 趋势上，平均每日发起横向威胁16.14万件；捕获次数最多的是8月9日，达51.46万次；波动最大的是8月24日，较8月23日减少92.56%；在8月1日至8月3日、8月7日至8月9日等出现连续3日以上的持续增长。在8月3日至8月7日、8月9日至8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4.88百万次，占总数的97.49%；其次是锐捷交换机（7.42万次，1.48%）、内网IP范围（4.97万次，0.99%）等。

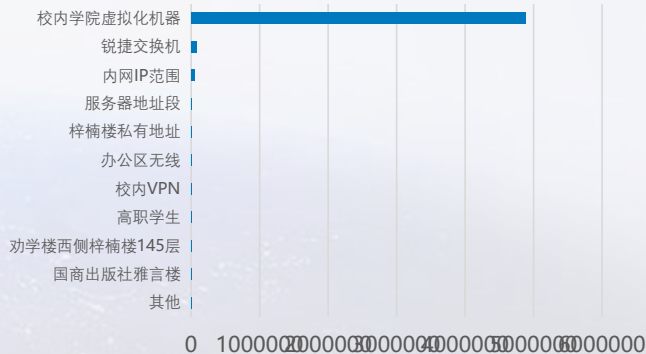
横向威胁类型分布



横向威胁趋势图



遭受横向威胁分支排行

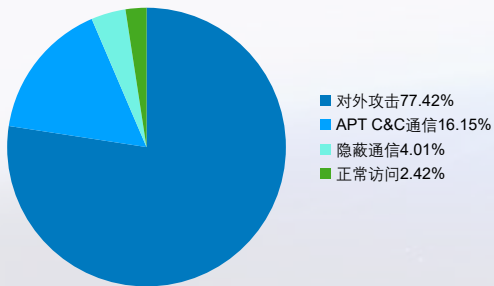




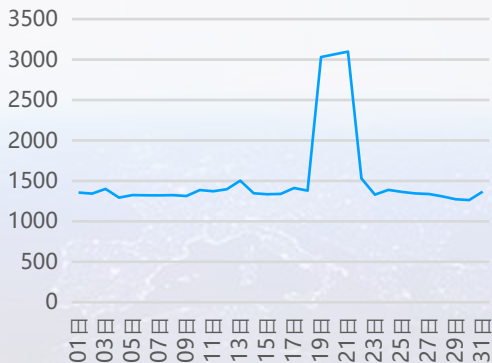
网络安全风险详情-外连威胁

- 在2026年08月共捕获外连威胁主机47台，外连威胁事件4.72万件，其中对外攻击排名第一，占比77.42%；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1521.68件；捕获次数最多的是8月21日，达3098次；波动最大的是8月19日，较8月18日增加119.64%；在8月11日至8月13日、8月15日至8月17日等出现连续3日以上的持续增长。在8月5日至8月7日、8月13日至8月15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、德国、菲律宾、日本，这5个国家/地区的外连次数占总体境外外连地区的99.95%；境内主要来源浙江、广东、北京、中国、上海，这5个省份的外连次数占总体外连次数99.13%，占总外连次数的20.93%；

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

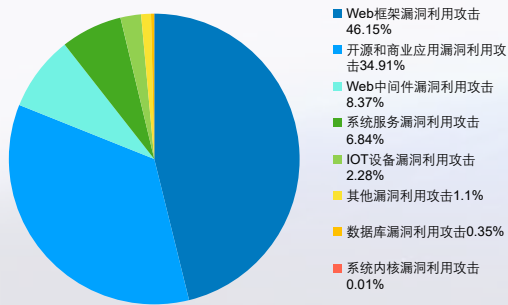




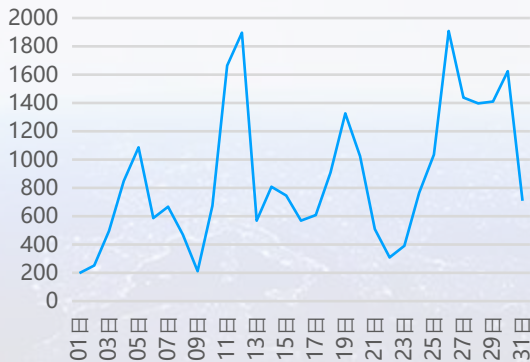
网络安全风险详情-漏洞利用

- 漏洞利用是最常见的一种网络攻击，2026年08月共捕获漏洞利用攻击告警2.71万次，其中Web框架漏洞利用攻击排名第一，占比46.15%；其次是开源和商业应用漏洞利用攻击、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874.32件；捕获次数最多的是8月26日，达1908次；波动最大的是8月13日，较8月12日减少69.99%；在8月1日至8月5日、8月9日至8月12日等出现连续3日以上的持续增长。在8月7日至8月9日、8月14日至8月16日等出现连续3日以上的持续减少。
- 按资产组分布，发生漏洞利用攻击最多的是服务器地址段，共1.12万次，占总数的45.2%；其次是校内学院虚拟化机器（1.03万次，41.35%）、内网IP范围（2482次，10.01%）等。

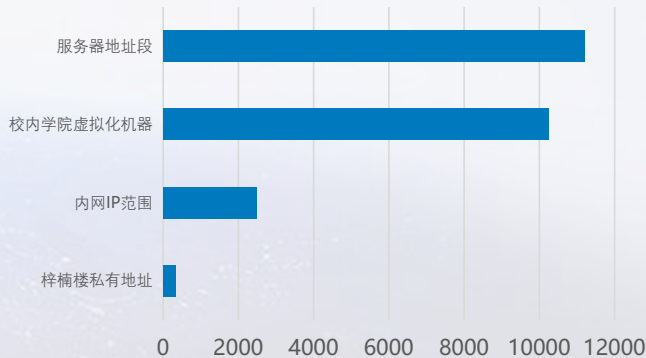
漏洞利用攻击类型



漏洞利用趋势图



遭受漏洞利用攻击分支排行





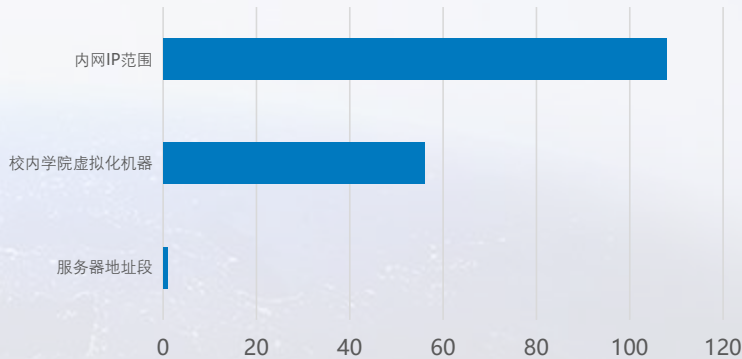
网络安全风险详情-文件安全

- 文件是病毒传播的常见手段；2026年08月共查杀文件687271余次，确认为恶意文件的有165个；
- 趋势上，平均每日捕获恶意文件5.32件；审计次数最多的是8月8日，达33次；波动最大的是8月5日，较8月4日减少100%；在8月8日至8月10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108次，占总数的65.45%；其次是校内学院虚拟化机器（56次，33.94%）、服务器地址段（1次，0.61%）等。

文件威胁趋势图



遭受文件安全分支排行

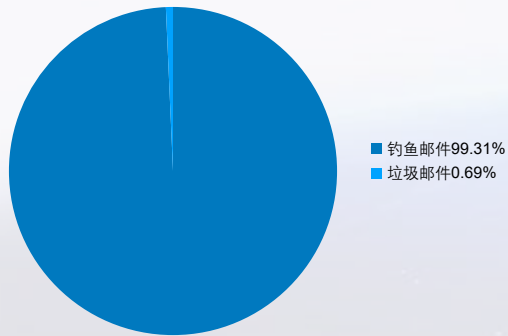




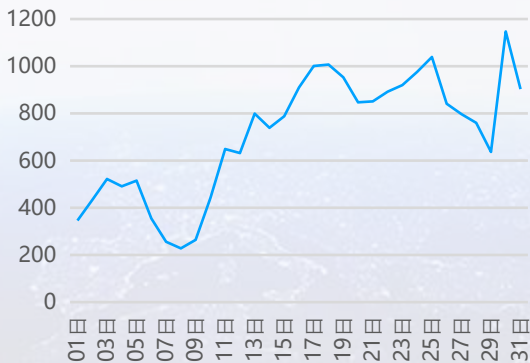
网络安全风险详情-邮件安全

- ♦ 邮件是恶意软件分发和网络钓鱼的头号媒介；2026年08月，共捕获钓鱼邮件99.31%21787次；垃圾邮件0.69%152次；
- ♦ 趋势上，平均每日捕获邮件安全风险707.71件；捕捉最高的是8月30日，达1147次；波动最大的是8月30日，较8月29日增加80.06%；在8月1日至8月3日、8月8日至8月11日等出现连续3日以上的持续增长。在8月5日至8月8日、8月18日至8月20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2.19万次，占总数的100%；

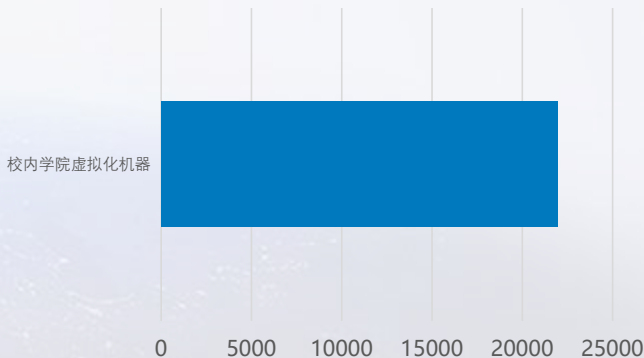
邮件安全风险分布



邮件安全趋势图



遭受邮件安全分支排行

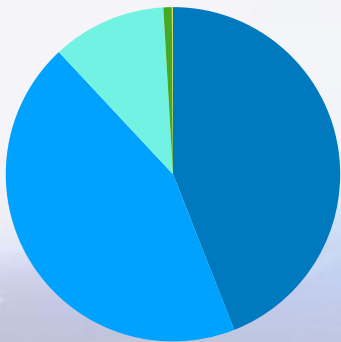




网络安全风险详情-暴力破解

- 暴力破解是最常见的一种网络攻击，2026年08月共捕获暴力破解攻击告警4.3百万次，其中其它口令暴力破解排名第一，占比44.03%;其次是口令暴力破解、SMTP账号暴力破解。
- 暴破频率最高达901次/分钟，该告警于2026年08月12日07时55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



- 其它口令暴力破解44.03%
- 口令暴力破解44.02%
- SMTP账号暴力破解11.03%
- IMAP账号暴力破解0.81%
- SSH账号暴力破解0.08%
- POP3账号暴力破解0.04%
- RDP账号暴力破解0%
- Web账号暴力破解0%



捕获时间: 2026-08-12 07:55:38
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。2026年08月共捕获漏洞0个，Web明文传输129个，配置错误风险329个，弱密码账号63个；
- 捕获最多的是-，共捕获0次，占有漏洞的0%；
- 平均每日捕获高危漏洞0个；捕获次数最多的是8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

漏洞

129个

Web明文传输

329个

配置风险

63个

弱密码

2026年08月漏洞态势



漏洞类型分布



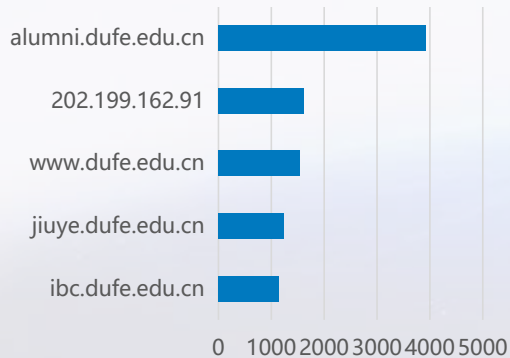
暂无数据



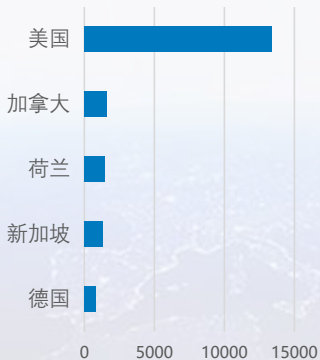
网络安全风险详情-网站攻击

- 2026年08月，共捕获网站类攻击4.93万次，其中被攻击最多的网站是alumni.dufe.edu.cn，达到3929次，占总体的7.97%；其次是202.199.162.91、www.dufe.edu.cn。
- 2026年08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、荷兰、新加坡、德国，这5个国家/地区的网站攻击占总体境外网站攻击的66.69%；境内主要来源辽宁、香港、浙江、重庆、台湾，这5个省份的网站攻击占总体境内网站攻击78.58%，占有网站攻击的34.13%；
- 趋势上，平均每日捕获网络攻击1590.58次；捕获次数最高的是8月26日，达4451次；波动最大的是8月26日，较8月25日增加388.05%；在8月13日至8月16日、8月17日至8月19日出现连续3日以上的持续增长。在8月5日至8月9日、8月19日至8月21日出现连续3日以上的持续减少。

排名前五的受攻击网站



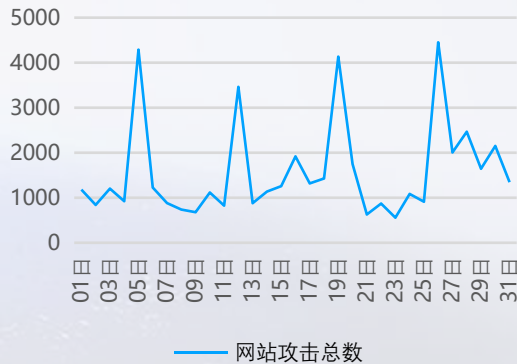
境外攻击源地区



境内攻击源地区



2026年08月网站攻击态势





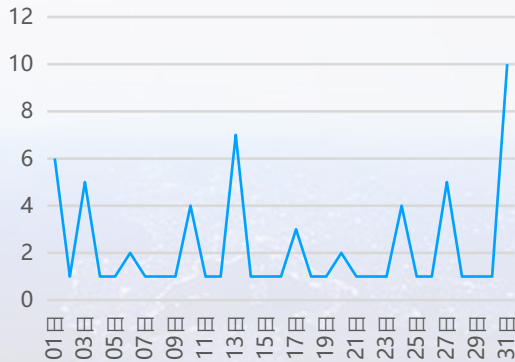
网络安全风险详情-僵尸网络

- 2026年08月，共捕获僵尸网络69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55.07%；排名第二第三的agent、xmrig比例分别为20.29%、20.29%
- 趋势上，平均每日捕获僵尸网络攻击2.23次；捕获次数最高的是8月31日，达10次；波动最大的是8月31日，较8月30日增加900%；
- 按资产组分布，发生僵尸网络最多的是内网IP范围，共33次，占总数的47.83%；其次是服务器地址段（30次，43.48%）、劝学楼西侧梓楠楼145层（2次，2.9%）等。

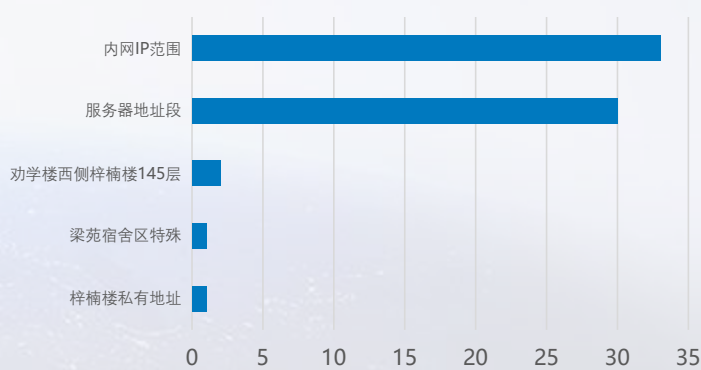
排名前五的僵尸网络家族



僵尸网络趋势图



遭受僵尸网络分支排行

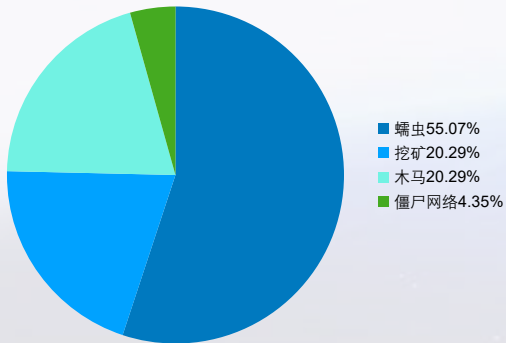




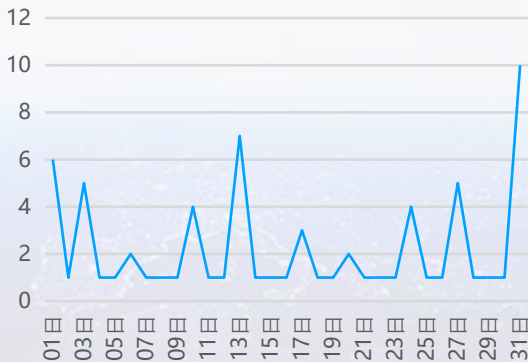
网络安全风险详情-有害程序

- 2026年08月，共捕获有害程序告警69次；其中最为活跃的是蠕虫，共捕获38次，占有恶意程序捕获数量的55.07%；而排名第二第三的挖矿、木马的比例分别为20.29%、20.29%
- 趋势上，平均每日捕获有害程序风险2.23次；捕获次数最高的是8月31日，达10次；波动最大的是8月31日，较8月30日增加900%；
- 按资产组分布，发生有害程序最多的是内网IP范围，共33次，占总数的47.83%；其次是服务器地址段（30次，43.48%）、劝学楼西侧梓楠楼145层（2次，2.9%）等。

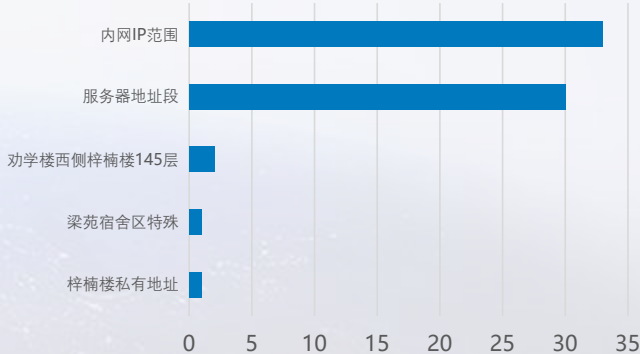
有害程序类型分布



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

2026年08月