



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09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2.99千万次,较上个月增加49.06%; 平均每日捕获攻击近99.51万次, 攻击者数量达9.05万个, 来源国家或地区168个, 境外主要来自美国、法国、新加坡, 境内主要是河北、山西、辽宁。外部攻击形势依旧严峻;
- 共捕获恶意程序事件490次; 网络攻击事件51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22个;

2.99千万次 ↑

攻击总数

9.05万个 ↓

攻击者

134个 ↓

境外攻击地区

490个 ↑

恶意程序事件

51个 ↑

网络攻击事件

17个 ↑

其他

0个

漏洞总数

22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



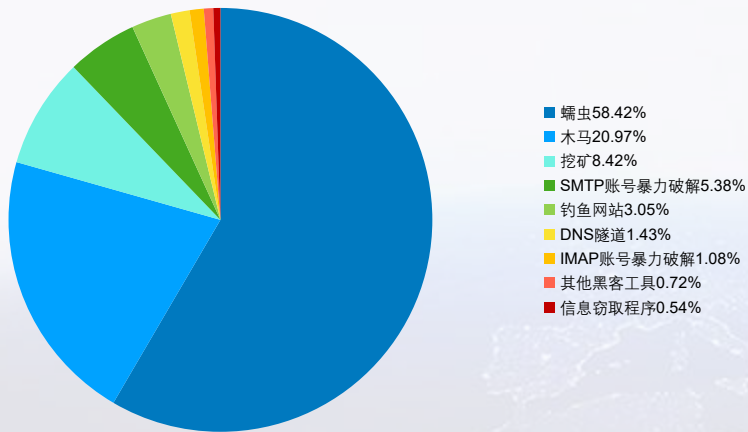
暂无数据



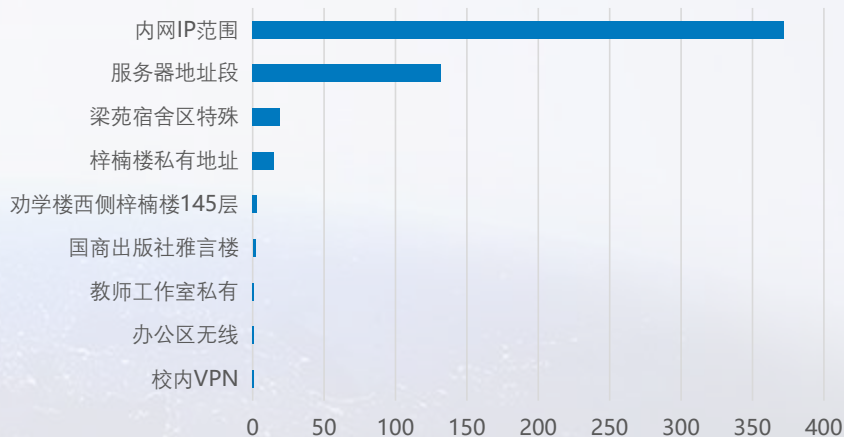
网络安全整体解读-安全总览

- 2026年09月最突出的安全风险前三名分别是蠕虫、木马、挖矿，本月处理这三类风险分别为58.42%、20.97%、8.42%，占本月总风险87.81%；针对这些风险，共处置主机117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372次，占总数的66.67%；其次是服务器地址段（132次，23.66%）、梁苑宿舍区特殊（19次，3.41%）；安全风险次数最少的是教师工作室私有、办公区无线、校内VPN。

2026年09月安全风险类型分布图



2026年09月资产组安全排行





网络安全整体解读-安全态势

- 2026年09月平均每日捕获风险资产16.37个左右，占总资产数（服务器208个、终端103108个）0.02%；风险资产总数在9月11日达到高峰，共85个，占资产总数0.08%；“已失陷”资产在9月9日增幅最大，增幅达2000%，从4个增加到84个；“已失陷”资产数在9月10日经过处置后，同比减少91.67%；“高危”资产数在9月8日经过处置后，同比减少100%；“安全”类资产在9月1日至9月3日、9月11日至9月14日出现连续3日以上的持续增长；“安全”类资产在9月26日至9月28日出现连续3日以上的持续减少；
- 2026年09月共捕获外部网络攻击2.99千万次，平均每日99.51万次；较上个月增加49.06%；在9月28日达到最高的1.24百万次；波动最大的是9月20日，较9月19日减少32.73%；在9月4日至9月6日、9月7日至9月9日等出现连续3日以上的持续增长。在9月2日至9月4日、9月9日至9月11日等出现连续3日以上的持续减少。

2026年09月整体资产安全态势



2026年09月网络攻击态势

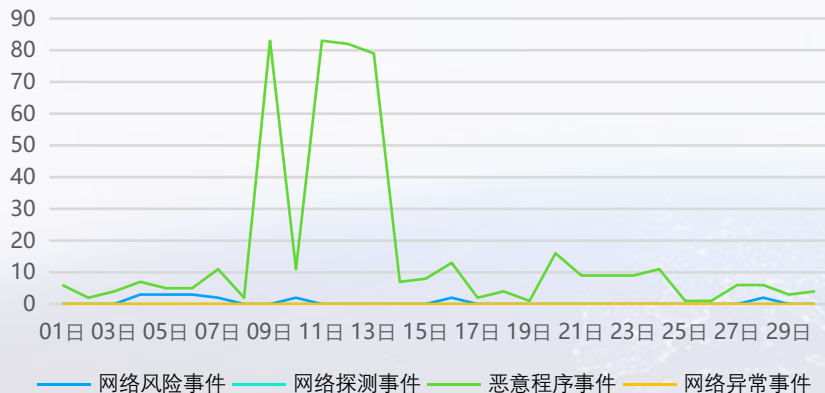




网络安全整体解读-安全态势

- 2026年09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558次，日均18.6次，其中9月9日最高83次；
- 2026年09月共捕获漏洞0个，平均每日0个；捕获次数最高的是9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9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09月非网络攻击类事件态势



2026年09月漏洞态势





网络安全整体解读-安全处置工作概览

- 2026年09月共处置风险主机136个，较上个月增加655.56%；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	2.99千万次	↑
	修复漏洞	0次	
	处置主机	136条	↑
	合规检查	0次	
	重大活动保障	0次	

2026年09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

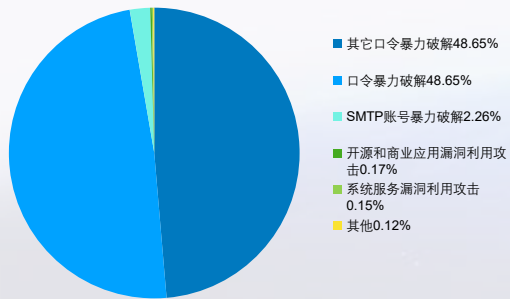
—— 本章节将详细阐述暴力破解、网站攻击、邮件安全、僵尸网络、恶意程序、业务脆弱性的捕获统计和趋势分析



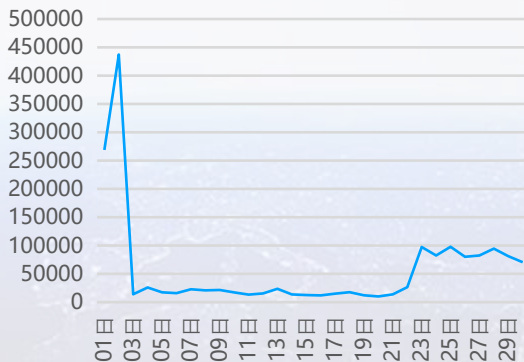
网络安全风险详情-横向威胁

- 在2026年09月共捕获横向威胁主机865台，横向威胁事件1.73百万件，其中其它口令暴力破解排名第一，占比48.65%；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5.78万件；捕获次数最多的是9月2日，达43.72万次；波动最大的是9月3日，较9月2日减少96.8%；在9月11日至9月13日、9月16日至9月18日等出现连续3日以上的持续增长。在9月4日至9月6日、9月9日至9月11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1.6百万次，占总数的92.28%；其次是锐捷交换机（7.22万次，4.17%）、内网IP范围（5.78万次，3.33%）等。

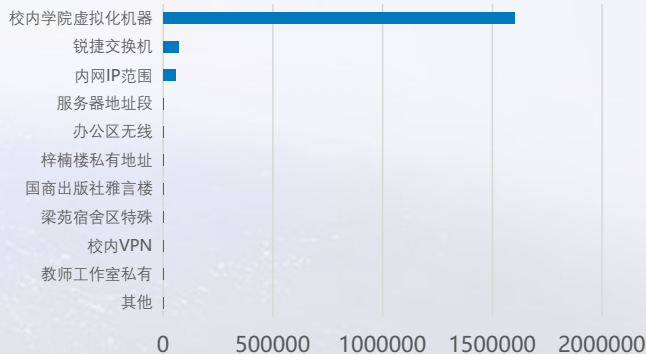
横向威胁类型分布



横向威胁趋势图



遭受横向威胁分支排行

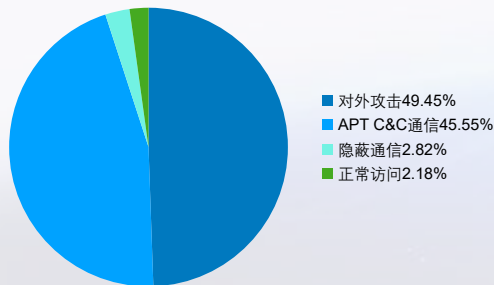




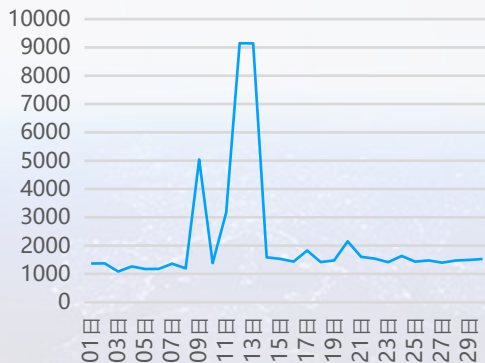
网络安全风险详情-外连威胁

- 在2026年09月共捕获外连威胁主机244台，外连威胁事件6.43万件，其中对外攻击排名第一，占比49.45%；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2143.17件；捕获次数最多的是9月12日，达9148次；波动最大的是9月14日，较9月13日减少82.65%；在9月5日至9月7日、9月10日至9月12日等出现连续3日以上的持续增长。在9月12日至9月16日、9月20日至9月23日出现连续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、日本、菲律宾、英国，这5个国家/地区的外连次数占总体境外外连地区的99.98%；境内主要来源北京、广东、浙江、辽宁、江苏，这5个省份的外连次数占总体外连次数93.35%，占总外连次数的9.59%；

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

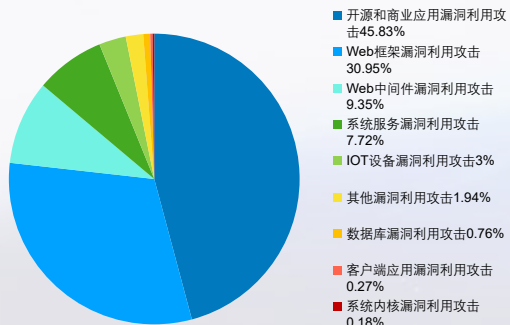




网络安全风险详情-漏洞利用

- 漏洞利用是最常见的一种网络攻击，2026年09月共捕获漏洞利用攻击告警2.66万次，其中开源和商业应用漏洞利用攻击排名第一，占比45.83%；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885.87件；捕获次数最多的是9月30日，达1900次；波动最大的是9月24日，较9月23日减少79.28%；在9月19日至9月23日、9月27日至9月30日出现连续3日以上的持续增长。在9月2日至9月4日、9月7日至9月11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1.05万次，占总数的49.45%；其次是校内学院虚拟化机器（6899次，32.36%）、内网IP范围（3140次，14.73%）等。

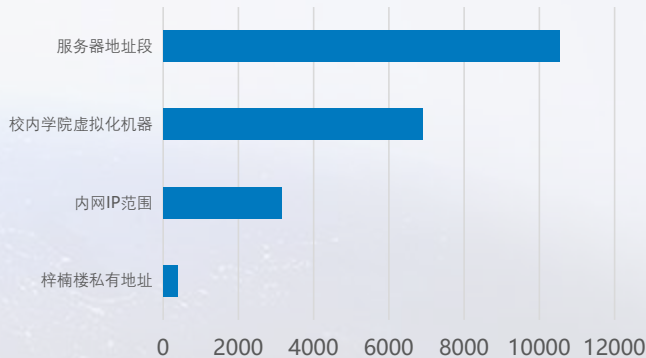
漏洞利用攻击类型



漏洞利用趋势图



遭受漏洞利用攻击分支排行

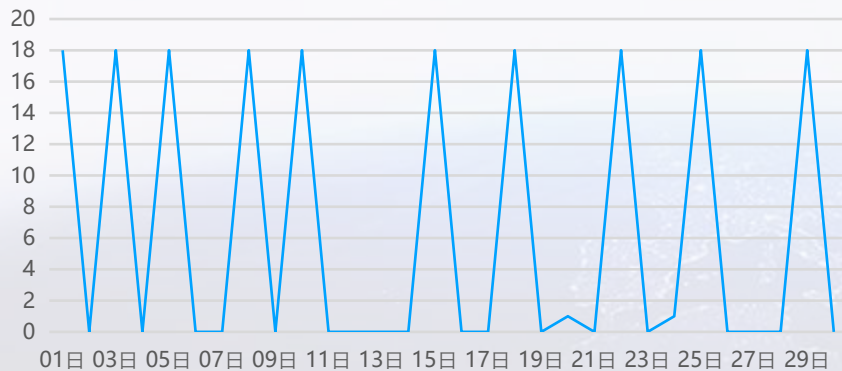




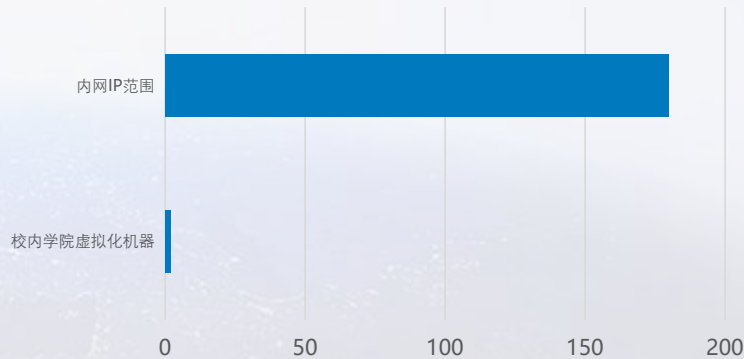
网络安全风险详情-文件安全

- 文件是病毒传播的常见手段；2026年09月共查杀文件6546279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6.07件；审计次数最多的是9月1日，达18次；波动最大的是9月2日，较9月1日减少100%；在9月23日至9月25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180次，占总数的98.9%；其次是校内学院虚拟化机器（2次，1.1%）等。

文件威胁趋势图



遭受文件安全分支排行

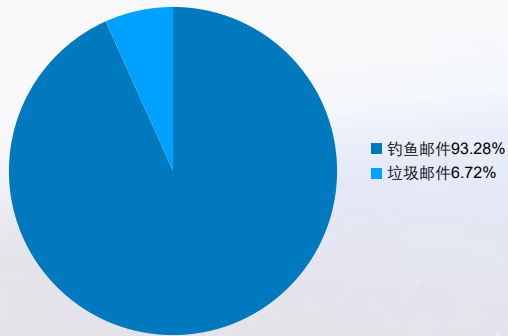




网络安全风险详情-邮件安全

- ♦ 邮件是恶意软件分发和网络钓鱼的头号媒介；2026年09月，共捕获钓鱼邮件93.28%4552次；垃圾邮件6.72%328次；
- ♦ 趋势上，平均每日捕获邮件安全风险162.67件；捕捉最高的是9月4日，达595次；波动最大的是9月8日，较9月7日增加931.25%；在9月7日至9月9日、9月15日至9月17日等出现连续3日以上的持续增长。在9月1日至9月3日、9月4日至9月7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4880次，占总数的100%；

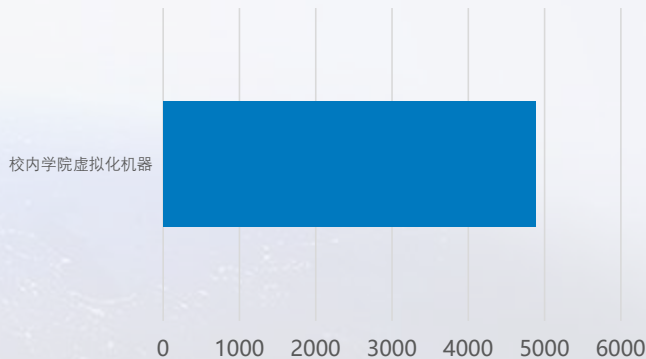
邮件安全风险分布



邮件安全趋势图



遭受邮件安全分支排行

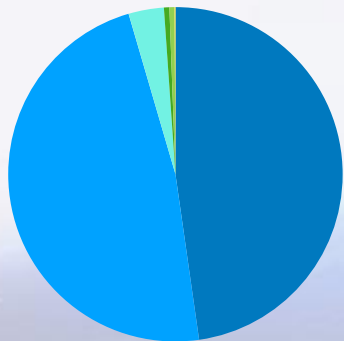




网络安全风险详情-暴力破解

- 暴力破解是最常见的一种网络攻击，2026年09月共捕获暴力破解攻击告警1.32百万次，其中口令暴力破解排名第一，占比47.74%;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09月01日03时44分捕获，来自于-攻击者118.202.165.11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



■ 口令暴力破解47.74%
■ 其它口令暴力破解47.74%
■ SMTP账号暴力破解3.41%
■ SSH账号暴力破解0.52%
■ IMAP账号暴力破解0.5%
■ POP3账号暴力破解0.09%
■ Web账号暴力破解0%



捕获时间: 2026-09-01 03:44:32
攻击者: 118.202.165.11 (-)
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09月共捕获漏洞0个，Web明文传输172个，配置错误风险323个，弱密码账号120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9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

172个

Web明文传输

323个

配置风险

120个

弱密码

2026年09月漏洞态势



漏洞类型分布



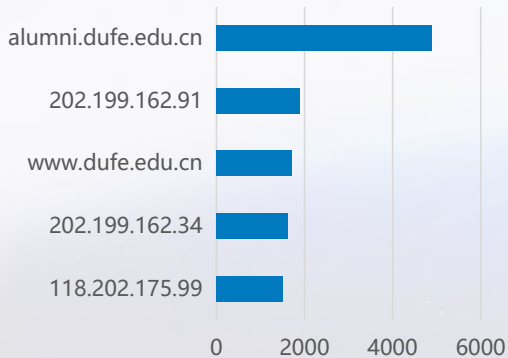
暂无数据



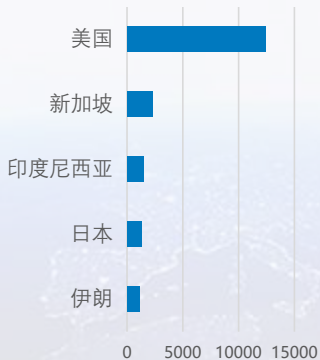
网络安全风险详情-网站攻击

- 2026年09月，共捕获网站类攻击5.21万次，其中被攻击最多的网站是alumni.dufe.edu.cn，达到4883次，占总体的9.37%；其次是202.199.162.91、www.dufe.edu.cn。
- 2026年09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、新加坡、印度尼西亚、日本、伊朗，这5个国家/地区的网站攻击占总体境外网站攻击的66.88%；境内主要来源辽宁、香港、台湾、浙江、山东，这5个省份的网站攻击占总体境内网站攻击85.61%，占有网站攻击的39.67%；
- 趋势上，平均每日捕获网络攻击1737.23次；捕获次数最高的是9月30日，达5311次；波动最大的是9月17日，较9月16日减少84.77%；在9月3日至9月5日、9月10日至9月12日出现连续3日以上的持续增长。在9月5日至9月8日、9月16日至9月18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



2026年09月网站攻击态势

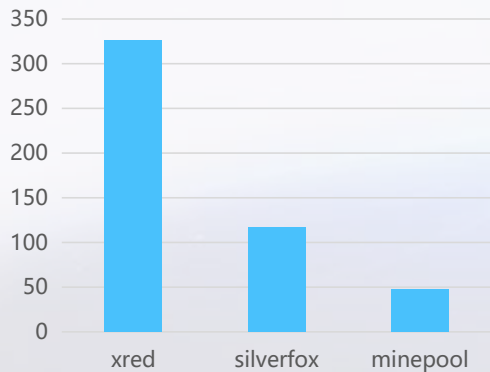




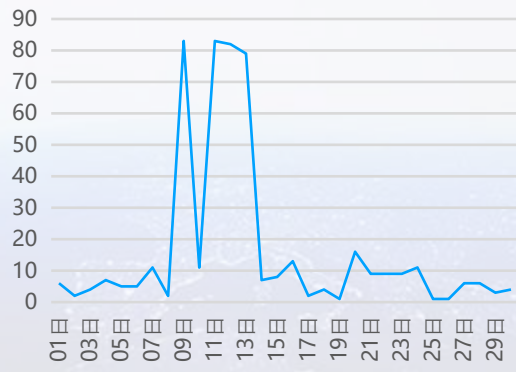
网络安全风险详情-僵尸网络

- 2026年09月，共捕获僵尸网络490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66.53%；排名第二第三的silverfox、minepool比例分别为23.88%、9.59%
- 趋势上，平均每日捕获僵尸网络攻击16.33次；捕获次数最高的是9月9日，达83次；波动最大的是9月9日，较9月8日增加4050%；在9月2日至9月4日、9月14日至9月16日出现连续3日以上的持续增长。在9月11日至9月14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内网IP范围，共357次，占总数的72.86%；其次是服务器地址段（84次，17.14%）、梁苑宿舍区特殊（19次，3.88%）等。

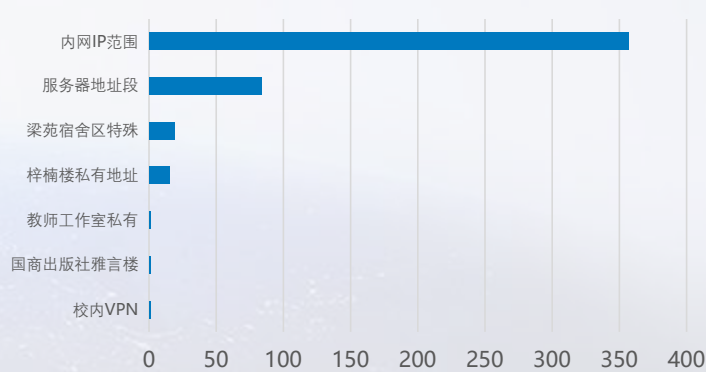
排名前五的僵尸网络家族



僵尸网络趋势图



遭受僵尸网络分支排行

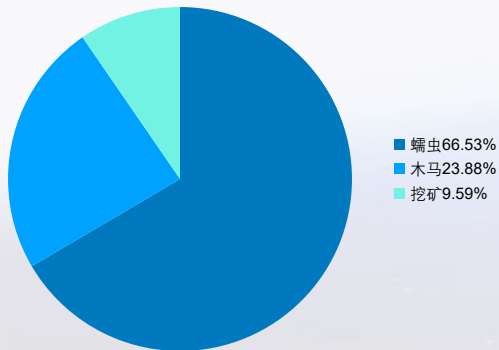




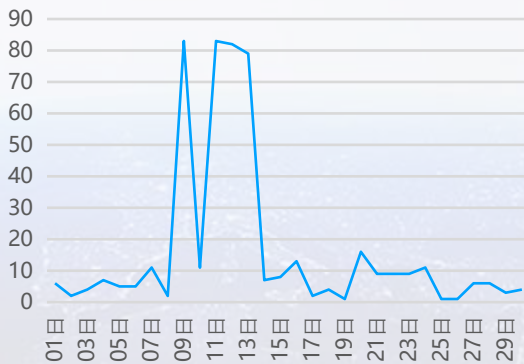
网络安全风险详情-有害程序

- 2026年09月，共捕获有害程序告警490次；其中最为活跃的是蠕虫，共捕获326次，占有恶意程序捕获数量的66.53%；而排名第二第三的木马、挖矿的比例分别为23.88%、9.59%
- 趋势上，平均每日捕获有害程序风险16.33次；捕获次数最高的是9月9日，达83次；波动最大的是9月9日，较9月8日增加4050%；在9月2日至9月4日、9月14日至9月16日出现连续3日以上的持续增长。在9月11日至9月14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内网IP范围，共357次，占总数的72.86%；其次是服务器地址段（84次，17.14%）、梁苑宿舍区特殊（19次，3.88%）等。

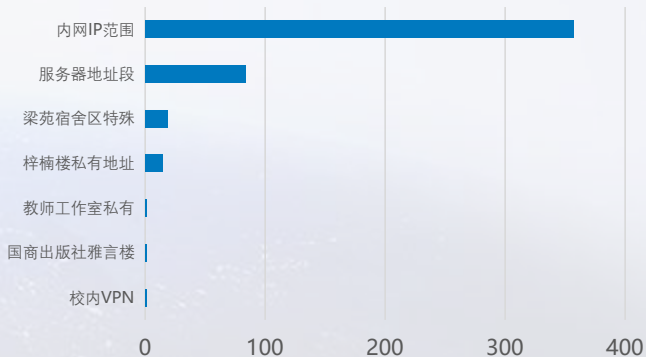
有害程序类型分布



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09月