安徽文达信息工程学院
网络信息中心
网络安全月报（二月）

报告类型： 网络安全

报告周期： 2026-02-01 09:33:00 - 2026-02-28 09:43:00

报告目录：

1. 网络及安全风险概况

- 总流量环比上月下降 91%，带宽未能有效利用。（假期使用人员减少）
- 活跃应用环比下降 14.07%，可能是正常情况，也可能是应用管控措施发挥了作用。
- URL 访问上个周期无高风险。
- 网络威胁环比下降 15.11%，安全处置措施有效，发挥了重大作用，网络安全情况得到有效改善。

网络概览

15.27 TB

设备总流量

网络应用

1191

个活跃应用

93

高风险应用

网络威胁

61021

网络攻击

3863

恶意软件

135

扫描

834

拒绝服务

73

网络钓鱼

0

垃圾邮件

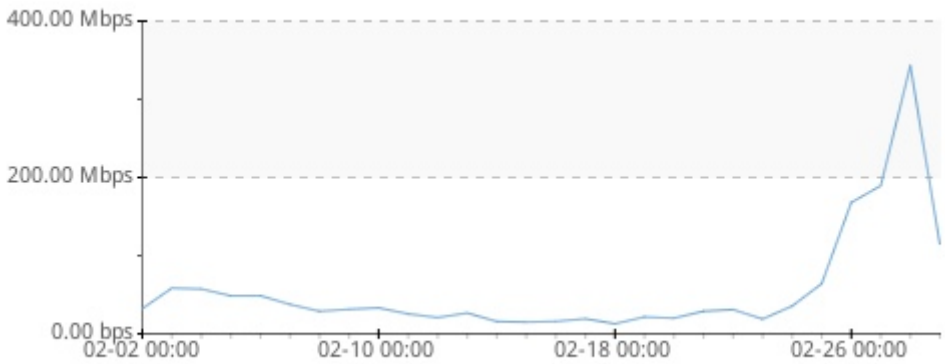
2. 网络流量详情

网络流量反映网络使用的整体情况，通过相关流量统计，能够有效了解链路带宽的利用情况，主要的访问去向，以及流量管理的健康程度。

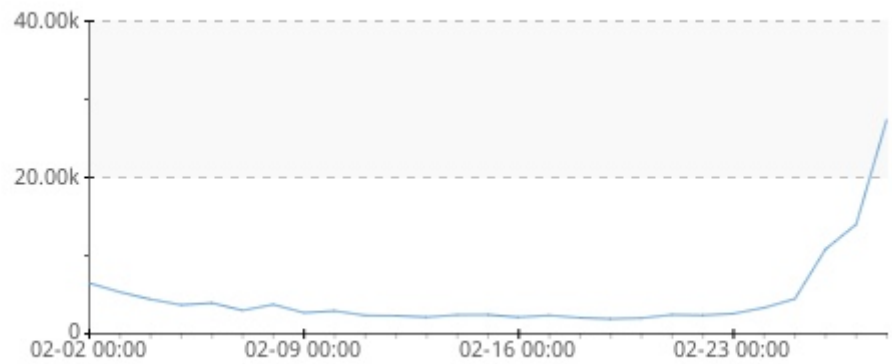
主要发现

- 统计期间整机平均流量 57.85 Mbps，峰值流量 342.98 Mbps，发生在 2026-02-28 00:00。
- 统计期间整机平均并发会话 4658，峰值并发会话 27457，发生在 2026-02-28 00:00。

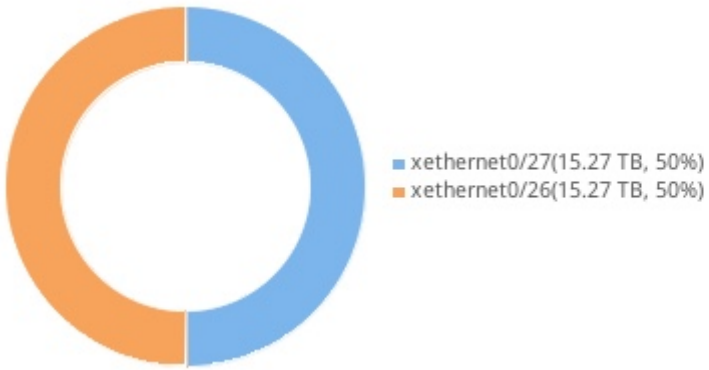
总流量趋势



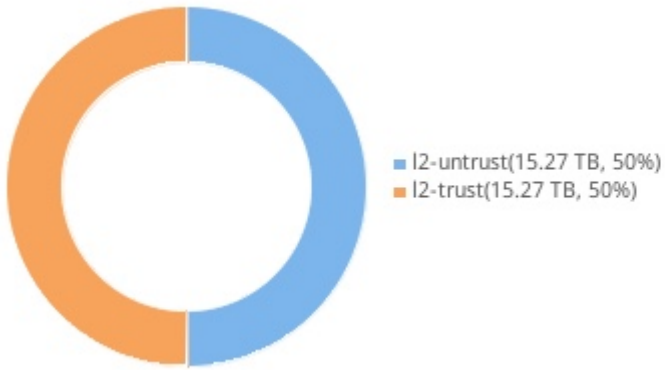
并发会话趋势



接口流量统计分布



安全域流量统计分布



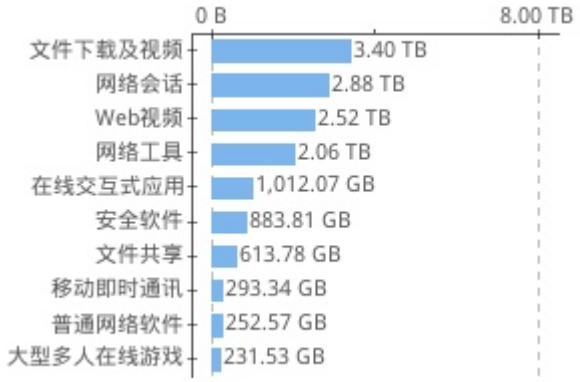
3. 应用统计及风险详情

应用程序可能会引入风险，例如病毒木马传播、传输敏感数据、消耗带宽。需要全面掌握内网的主要业务应用使用情况，根据实际的网络环境状态进行有效调整。

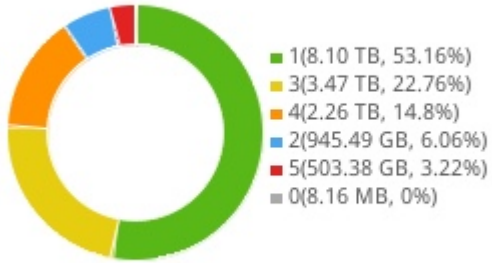
主要发现

- 总共使用 1191 款应用程序，会造成潜在的业务和安全挑战。这是因为关键功能转向外部而不受企业控制，员工使用与工作无关的应用程序，或者网络攻击者使用这些应用程序来传输威胁和窃取数据。
- 在网络上发现了诸如 HTTPS,HTTP,HTTP 分片下载等高风险应用程序，由于存在滥用的可能性，应予以调查。

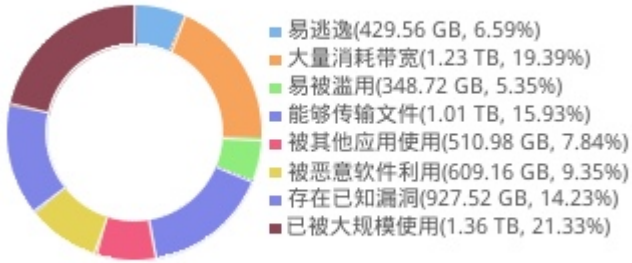
应用子类别排名



应用风险等级分布



应用特征分布



应用列表 TOP10

风险等级	应用名称	应用子类别	应用技术	总流量
1	UDP 下载及视频	文件下载及视频	网络协议	2.61 TB
4	HTTPS	网络会话	基于浏览器	1.68 TB
1	抖音短视频	Web 视频	客户端服务器	1.65 TB
1	UDP 交互式应用	在线交互式应用	网络协议	1,008.87 GB
3	Windows 自动更新	安全软件	客户端服务器	854.62 GB
1	TCP 下载及视频	文件下载及视频	网络协议	808.72 GB
1	腾讯网	网络工具	客户端服务器	633.46 GB
3	百度网盘	文件共享	客户端服务器	432.63 GB
3	腾讯视频	Web 视频	基于浏览器	309.89 GB
5	HTTP	网络会话	网络协议	305.01 GB

4. URL 活动及风险详情

Web 是网络威胁入侵的途径之一，高风险的网站访问极易带来安全隐患，热门网站类型的访问能够体现网络行为的基本情况和整体状态，了解网络带宽的主要应用，避免无谓的带宽消耗。

主要发现

- 本月未发现高风险 URL 活动。

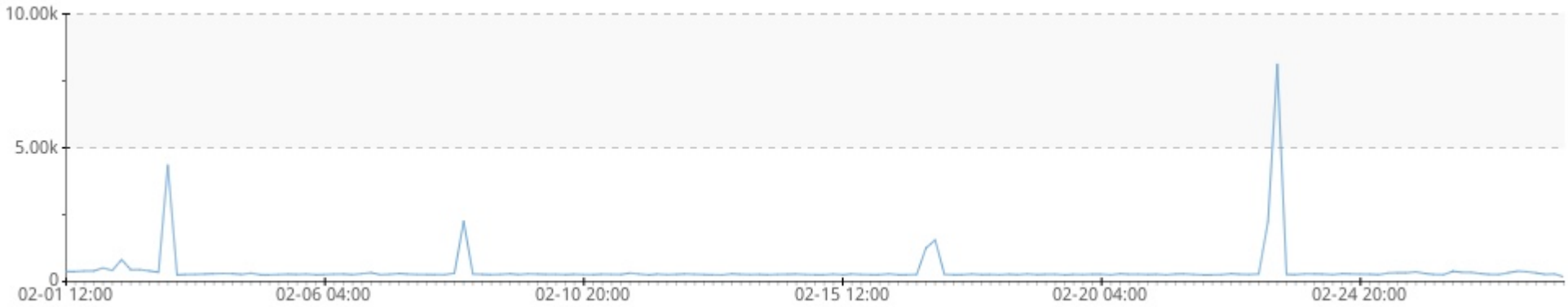
5. 网络风险威胁详情

网络入侵攻击、APT 攻击、网络钓鱼、垃圾邮件、网络传播病毒木马统称为网络威胁，通过了解当前网络中存在的网络威胁，以掌握网络风险程度，并根据具体情况采取相应的安全处置措施。

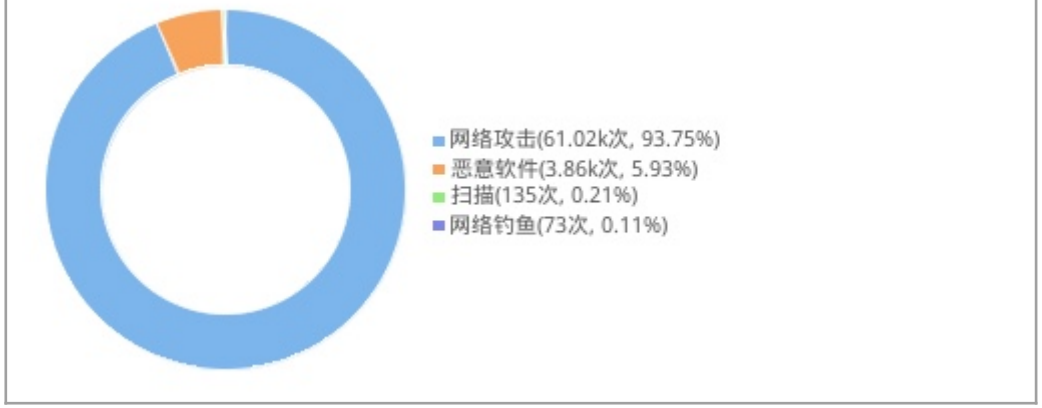
主要发现

- 周期内共产生 65092 次威胁行为，其中网络攻击占比 93.75%，恶意软件占比 5.93%，扫描占比 0.21%。
- 2026-02-23 04:00 至 2026-02-23 08:00 为威胁高发期，发生网络攻击，恶意软件等威胁行为，总计 8116 次。

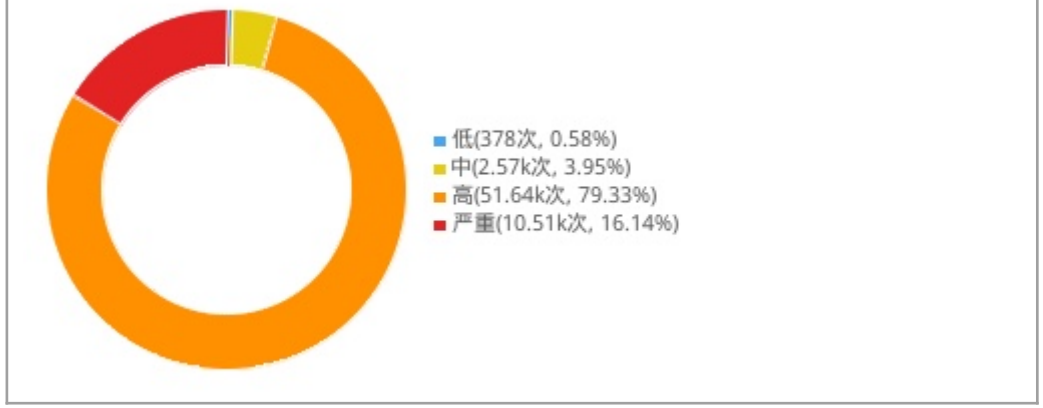
威胁趋势图



威胁类型分布

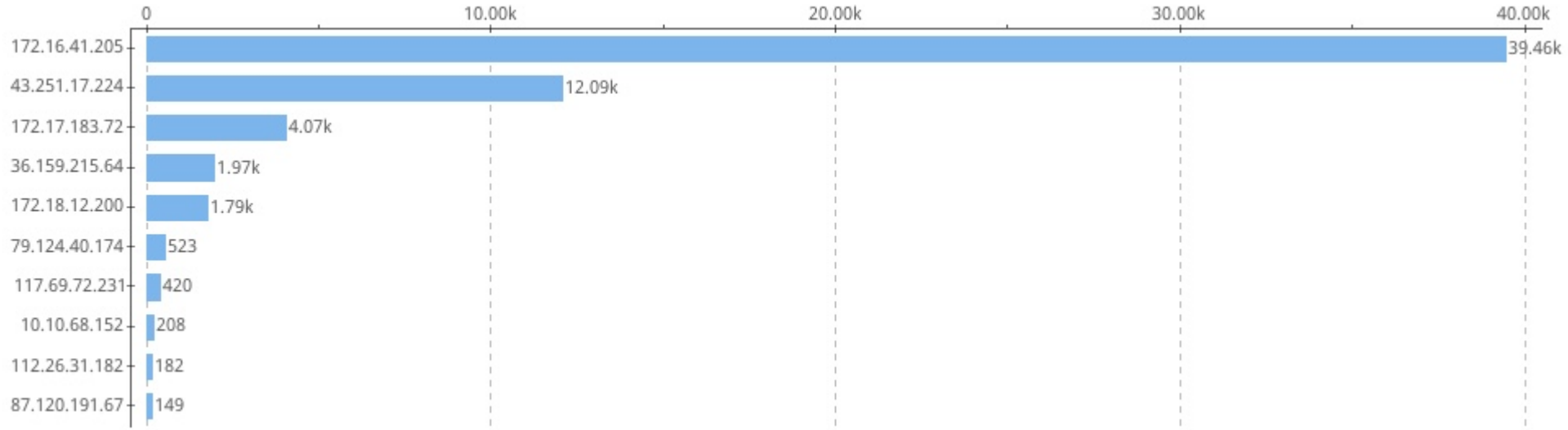


威胁严重程度分布

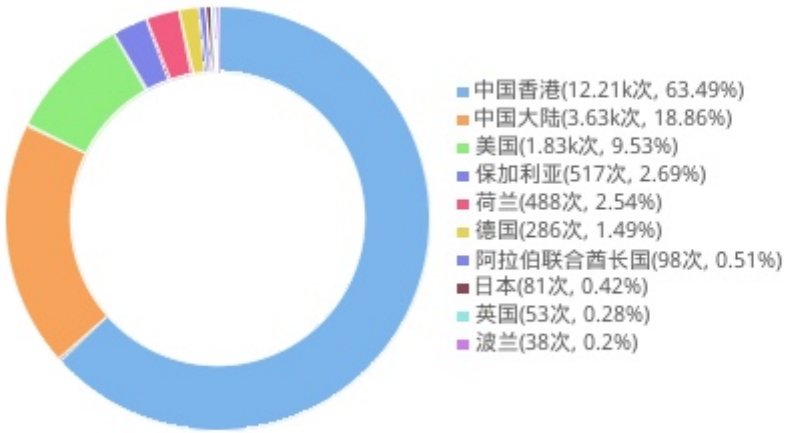


5. 网络风险威胁详情

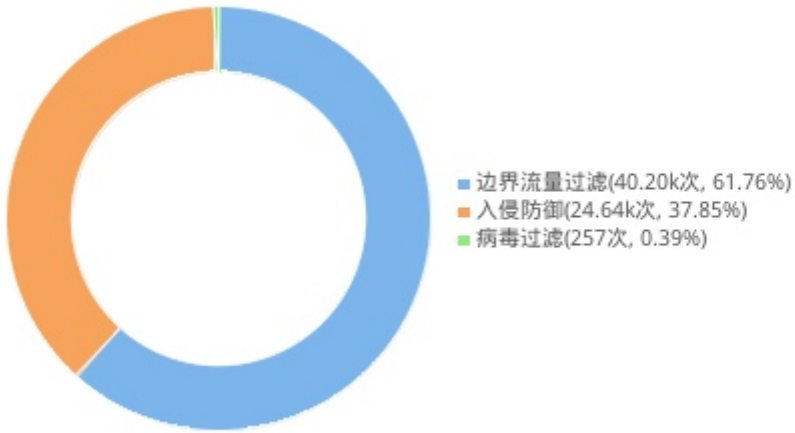
威胁攻击源排名



外部攻击地理分布



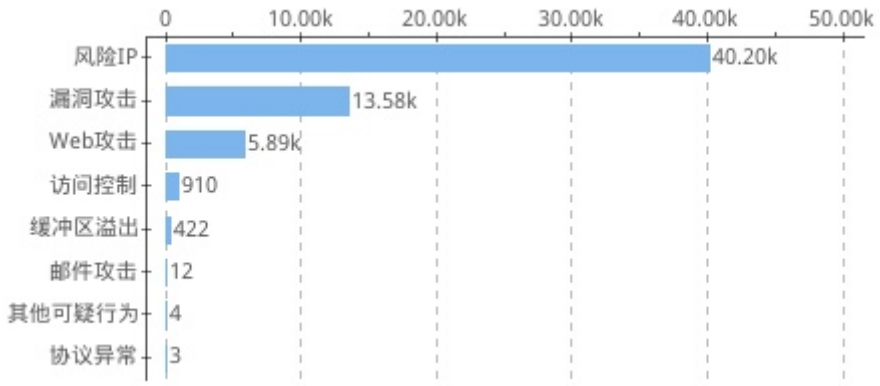
威胁检测引擎分布



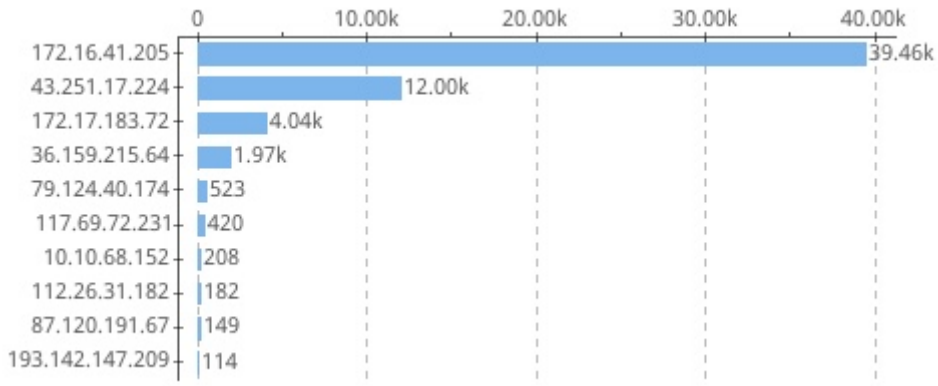
5. 网络风险威胁详情

发现 8 种网络攻击类型，其中风险 IP 占比 65.88%，漏洞攻击占比 22.26%，Web 攻击占比 9.65%。

网络攻击类型排名

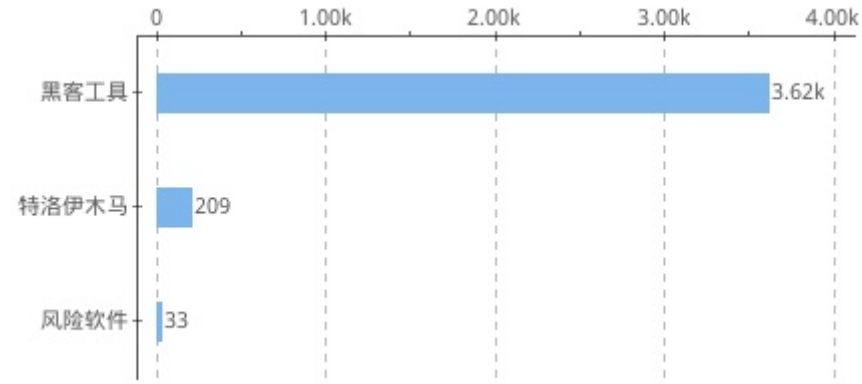


网络攻击类型攻击源排名

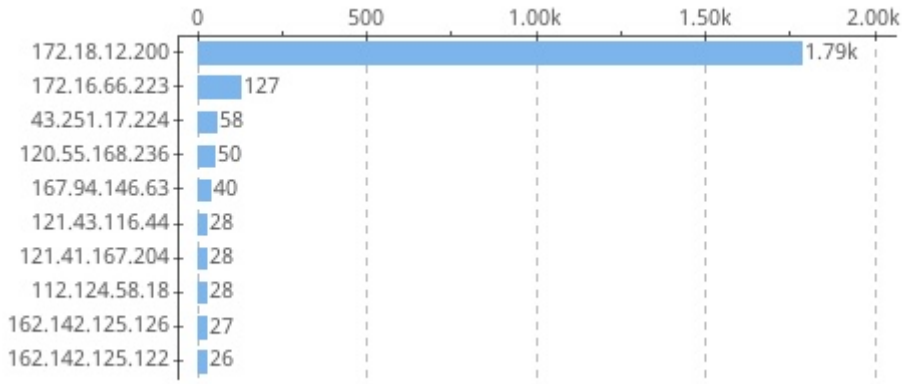


发现 3 种恶意软件类型，其中黑客工具占比 93.74%，特洛伊木马占比 5.41%，风险软件占比 0.85%。

恶意软件类型排名



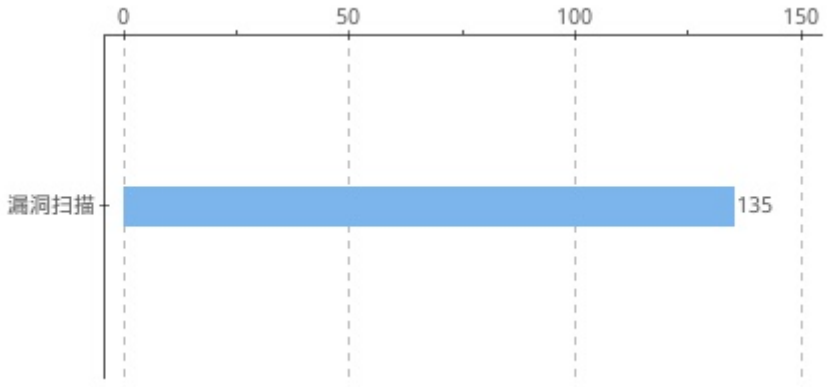
恶意软件类型攻击源排名



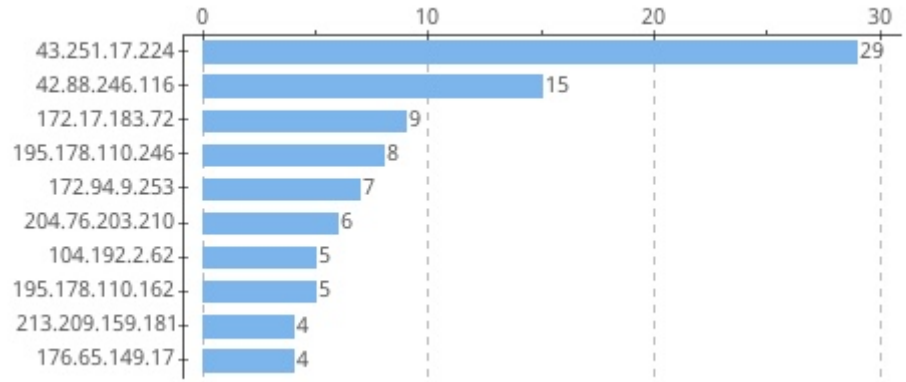
5. 网络风险威胁详情

发现 1 种扫描类型，其中漏洞扫描占比 100%。

扫描类型排名

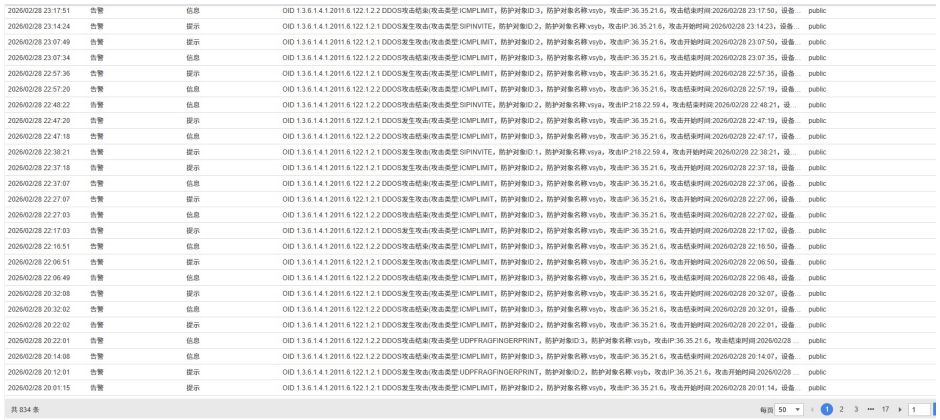


扫描类型攻击源排名



发现拒绝服务 834 次。

拒绝服务类型排名



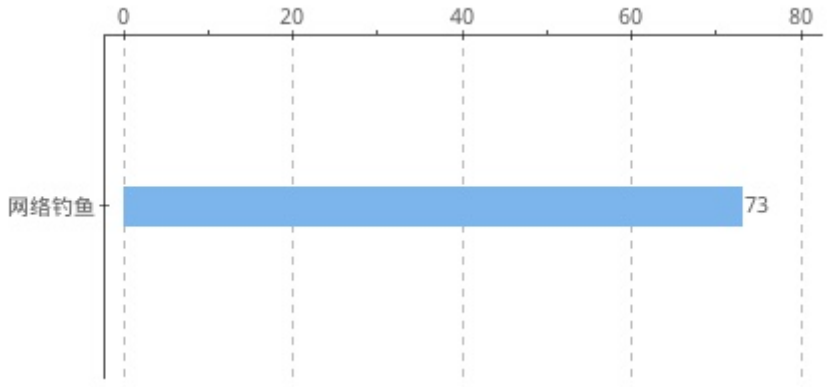
2026/02/28 23:17:51	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 23:17:50，设备...	public
2026/02/28 23:14:24	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:SIPINVITE，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 23:14:23，设备...	public
2026/02/28 23:07:49	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 23:07:50，设备...	public
2026/02/28 23:07:34	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 23:07:35，设备...	public
2026/02/28 22:57:36	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 22:57:35，设备...	public
2026/02/28 22:57:20	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 22:57:19，设备...	public
2026/02/28 22:48:22	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:SIPINVITE，防护对象ID:2，防护对象名称:vsya，攻击IP:218.22.59.4，攻击结束时间:2026/02/28 22:48:21，设...	public
2026/02/28 22:47:20	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 22:47:19，设备...	public
2026/02/28 22:47:18	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 22:47:17，设备...	public
2026/02/28 22:38:21	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:SIPINVITE，防护对象ID:1，防护对象名称:vsya，攻击IP:218.22.59.4，攻击开始时间:2026/02/28 22:38:21，设...	public
2026/02/28 22:37:18	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 22:37:18，设备...	public
2026/02/28 22:37:07	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 22:37:06，设备...	public
2026/02/28 22:27:07	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 22:27:06，设备...	public
2026/02/28 22:27:03	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 22:27:02，设备...	public
2026/02/28 22:17:03	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 22:17:02，设备...	public
2026/02/28 22:16:51	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 22:16:50，设备...	public
2026/02/28 22:06:51	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 22:06:50，设备...	public
2026/02/28 22:06:49	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 22:06:48，设备...	public
2026/02/28 20:32:08	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 20:32:07，设备...	public
2026/02/28 20:32:02	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 20:32:01，设备...	public
2026/02/28 20:22:02	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 20:22:01，设备...	public
2026/02/28 20:22:01	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:UDPFRAGFINGERPRINT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28...	public
2026/02/28 20:14:08	告警	信息	OID 1.3.6.1.4.1.2011.6.122.1.2.2 DDOS攻击结束(攻击类型:ICMPLIMIT，防护对象ID:3，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击结束时间:2026/02/28 20:14:07，设备...	public
2026/02/28 20:12:01	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:UDPFRAGFINGERPRINT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28...	public
2026/02/28 20:01:15	告警	提示	OID 1.3.6.1.4.1.2011.6.122.1.2.1 DDOS发生攻击(攻击类型:ICMPLIMIT，防护对象ID:2，防护对象名称:vsyb，攻击IP:36.35.21.6，攻击开始时间:2026/02/28 20:01:14，设备...	public

共 834 条　　每页 50　‹ 1 2 3 ••• 17 ›　1

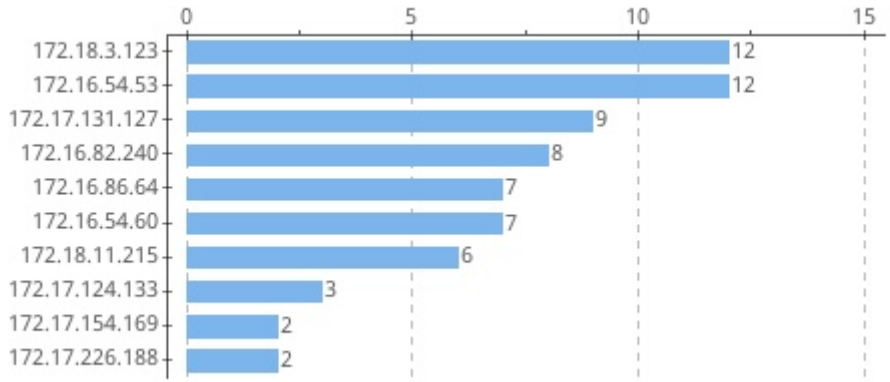
5. 网络风险威胁详情

发现 1 种网络钓鱼类型，其中网络钓鱼占比 100%。

钓鱼网站次数



钓鱼网站类型攻击源排名



未发现垃圾邮件。

垃圾邮件次数

没有数据

垃圾邮件类型攻击源排名

没有数据

6. 威胁说明

网络攻击

通过网络针对计算机软件系统、硬件系统、网络系统，以破坏信息系统的保密性、完整性、可用性、真实性和可控性为目的的行为，被称为网络攻击。网络攻击被分为：

WEB 攻击：随着 Web2.0、社交网络等一系列新型的互联网产品的诞生，基于 Web 环境的互联网应用越来越广泛，企业信息化的过程中各种应用都架设在 Web 平台上。Web 业务的迅速发展也引起黑客们的强烈关注，接踵而至的就是 Web 安全威胁的凸显，黑客利用网站操作系统的漏洞和 Web 服务程序的漏洞等得到 Web 服务器的控制权限，轻则篡改网页内容，重则窃取重要内部数据。此外，更为严重的是攻击者可以在网页中植入恶意代码，使得网站访问者受到侵害。常见的 Web 攻击有：1) SQL 注入攻击 2) 跨站脚本攻击(XSS) 3) 跨站请求伪造攻击(CSRF) 4) 目录遍历攻击 5) 网站信息泄露 6) 网页挂马 7) 服务器 Web Shell 挂马 8) Web 口令暴力破解 9) HTTP DDoS 攻击(CC 攻击) 10) 网页篡改

密码攻击：攻击者攻击目标时常常把破译用户的口令作为攻击的开始。只要攻击者能猜测或者确定用户的口令，他就能获得机器或者网络的访问权，并能访问到用户能访问到的任何资源。如果这个用户有域管理员或 root 用户权限，这是极其危险的。常见的密码攻击有： 1) 针对弱加密算法的攻击，例如 WEP WLAN 密码攻击 2) 穷举法密码暴力破解 3) 字典法密码暴力破解 4) 社会工程学密码破解等

网络欺诈：这是一种严重的攻击形式，攻击者借用另外一台正常主机的信息，从而冒充另外一台机器与服务器通信。常见的 Spoofing 攻击有：1) IP Spoofing：行动产生的 IP 数据包为伪造的源 IP 地址，以便冒充其他系统或发件人的身份。 2) ARP Spoofing：攻击者通过恶意 ARP 广播，将自己的 MAC 地址与被仿冒的主机 IP 地址进行绑定，以污染内网主机的 ARP 缓存。将所有到被仿冒主机的流量都牵引到攻击者主机。 3) DNS Spoofing：攻击者冒充域名服务器让目标主机把域名转换成错误 IP，其目的是让受害主机把通过域名查询到的 IP 地址设为攻击者所控制主机的 IP 地址。 4) WLAN Spoofing：攻击者通过仿冒受害者的无线 MAC 地址，从而代替受害者进行 WLAN 通信。

网络劫持：劫持攻击是一种网络攻击手段，攻击者可以通过破坏已建立的数据流而实现身份伪造并进行会话劫持。常见的劫持攻击有：1) TCP 劫持：通过侦测 TCP 序列号，通过模仿被劫持主机的 TCP/IP 序列号模仿被劫持主机的通信，而达到劫持的效果。 2) DNS 域名劫持：通过仿造 DNS 域名拥有者的身份信息，从而篡改域名信息、解析的地址，而达到盗窃域名所有权的后果。 3) 基于代理的中间人攻击：通过使用代理服务器，在受害者的通信过程中可以监视或篡改受害者的通信信息。 4) HTTP 会话劫持：HTTP 会话信息通常使用 Cookie 存储。攻击者通过类似 XSS 攻击的手段，可以偷取用户的身份令牌。在身份令牌的有效期内，攻击者可以通过重放令牌的手段冒用受害者的身份。 劫持攻击的主要危害有： 1) 嗅探敏感信息，例如受身份认证保护的涉密文件、信用卡密码等。 2) 冒用管理员身份查看、修改系统关键信息，例如 passwd 文件等。

协议异常：目前多数网络攻击都是通过通信协议完成的，入侵引起的异常也表现为协议的异常，作为异常检测新的发展方向，协议异常检测对协议的正常数据建模，检测违反协议规定的行为和异常数据。

访问控制：访问控制是指用户身份及其所归属的某项定义组来限制用户对某些信息项的访问，或限制对某些控制功能的使用的一种技术。该技术目的在于防止对任何资源进行未授权的访问，从而使计算机系统在合法的范围内使用。访问控制通常用于系统管理员控制用户对服

务器、目录、文件等网络资源的访问。 攻击者通常利用软件漏洞、弱口令探测、字典攻击、对认证服务器攻击等方式进行身份欺骗和绕过，从而可以访问受控制的资源。

恶意软件

恶意软件通常是指带有攻击意图的一段程序，主要包括：后门/木马，计算机病毒，计算机蠕虫，广告软件、黑客工具、间谍软件和风险软件。

扫描

扫描是一种是用扫描器完成的信息收集工作。在正式进行各种攻击行为之前，攻击者会采取各种手段，侦察对方的主机信息，以便决定使用何种最有效的方法达到自己的目的。攻击者通常使用扫描器来完成这个工作。扫描器是一类自动检测本地或远程主机安全弱点的程序，它能够快速的准确的发现扫描目标存在的漏洞并提供给使用者扫描结果。工作原理是扫描器向目标计算机发送数据包，然后根据对方反馈的信息来判断对方的操作系统类型、开发端口、提供的服务等敏感信息。

拒绝服务

DoS/DDoS 攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。这种攻击会导致资源的匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快都无法避免这种攻击带来的后果。 常见的 DoS 攻击有：Smurf 攻击、TearDrop 攻击等等；常见的 DDoS 攻击有 TCP Syn Flood 攻击、TCP ACK Flood 攻击、ICMP Flood 攻击、HTTP CC 攻击、DNS 反射攻击等。 要避免系统免受 DoS 攻击，网络管理员要积极谨慎地维护系统，确保无安全隐患和漏洞；而针对 DDOS 恶意攻击则需要安装防火墙等安全设备来过滤，同时应当定期查看安全设备的日志，及时发现对系统的安全威胁行为。

网络钓鱼

Phishing 与钓鱼的英语 fishing 发音相近，又名钓鱼式攻击。攻击者利用欺骗性的电子邮件和伪造的 Web 站点来进行网络诈骗活动，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。诈骗者通常会将自己伪装成网络银行、在线零售商和信用卡公司等可信的品牌，骗取用户的私人信息。 中国互联网络信息中心联合国家互联网应急中心发布的《中国网民网络信息安全状况调查报告》显示，近年来年有超过九成网民遇到过网络钓鱼。在遭遇过网络钓鱼事件的网民中，有超过 4000 万网民蒙受了经济损失，占网民总数 10%以上。网络钓鱼给网民造成的损失已超过 100 亿元人民币。

垃圾邮件

垃圾邮件一般具有批量发送的特征。其内容包括赚钱信息、成人广告、商业或个人网站广告、电子杂志、连环信等。垃圾邮件可以分为良性和恶性的。良性垃圾邮件是各种宣传广告等对收件人影响不大的信息邮件。恶性垃圾邮件是指具有破坏性的电子邮件。例如具有攻击性的广告：夸张不实，包括情色、钓鱼网站。有些垃圾邮件发送组织或是非法信息传播者，为了大面积散布信息，常采用多台机器同时巨量发送的方式攻击邮件服务器，造成邮件服务器大量带宽损失，并严重干扰邮件服务器进行正常的邮件递送工作。