山西省
煤炭能源、钢铁冶金、电力行业
11月份网络安全态势分析

2022年12月

11月份，我局依托现有技术手段对省内公共互联网进行持续监测，我省公用通信网和公共互联网基础网络运行状况整体正常，未发生造成较大影响的网络运行故障，未发生三级以上网络安全事件。现就我省煤炭能源、钢铁冶金、电力行业进行网络安全态势分析。

一、网络安全基本态势

（一）网络安全总体态势

11月份，通过对我省煤炭能源、钢铁冶金、电力行业遭受的网络攻击行为进行监测分析，发现70家企业（95个互联网主机）疑似遭受网络攻击（其中煤炭能源50家企业69个互联网主机，钢铁冶金9家企业11个互联网主机，电力行业11家企业14个互联网主机），环比下降9.09%（互联网主机环比下降25.19%），累计触发相关网络威胁告警18137条，环比下降71.06%。其中作为被攻击方遭受恶意网络攻击触发威胁告警16917次，作为木马、僵尸程序控制端对外进行恶意通信触发威胁告警1220次。

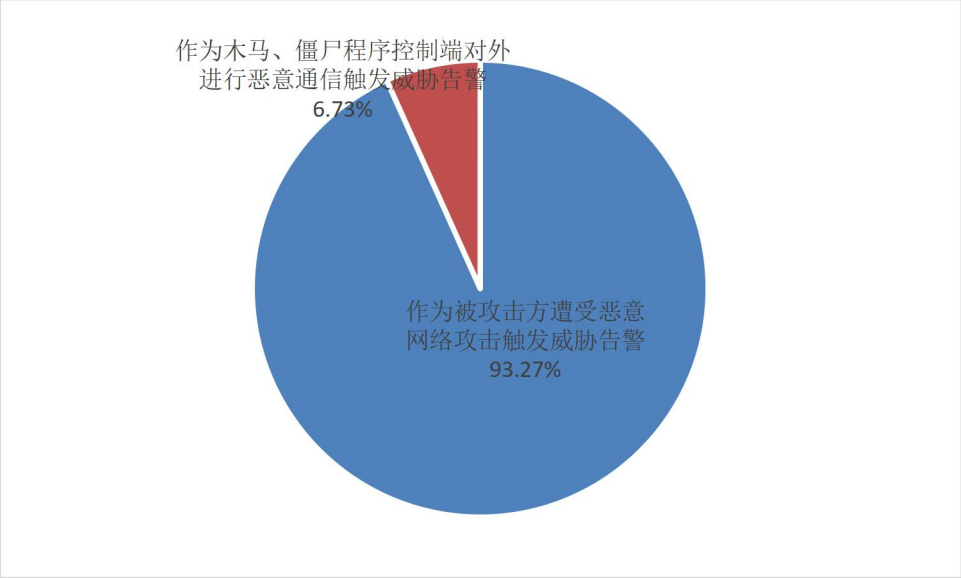

图 1 触发相关网络威胁告警分布及占比

（二）恶意网络资源传播是面临的主要威胁

11 月份，通过对我省煤炭能源、钢铁冶金、电力行业企业网络通信行为分析研判，结合第三方威胁情报库比对，由恶意资源传播触发网络威胁告警 10249 余次，其中被访问的恶意网络资源（恶意域名和恶意 IP） 包含:*.jifr.*、*.beahh.com、fget-career.com 等，主要为恶意程序及僵木蠕病毒传播源及远程控制端。

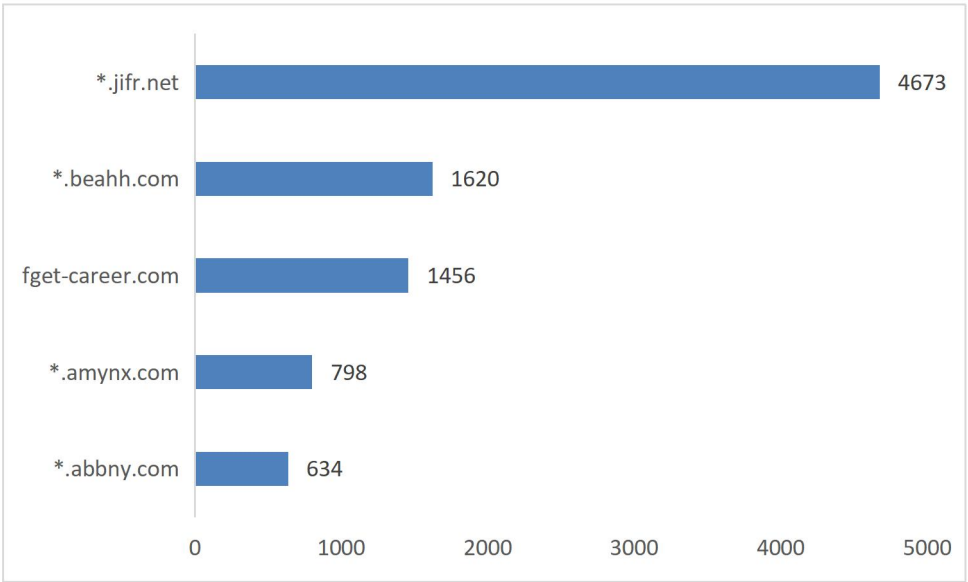

图 2 恶意域名和恶意 IPTOP5

（三）源自境外的恶意网络攻击活跃

11 月份，通过对我省煤炭能源、钢铁冶金、电力行业企业网络通信行为分析研判，结合第三方威胁情报库比对，由境外 IP 引发的网络威胁告警共 10947 次，占网络威胁告警总数的 60.36%。境外网络攻击的 IP 主要归属于比利时、美国、荷兰等国家，分别占比 40.54%、33.88%和 16.27%。

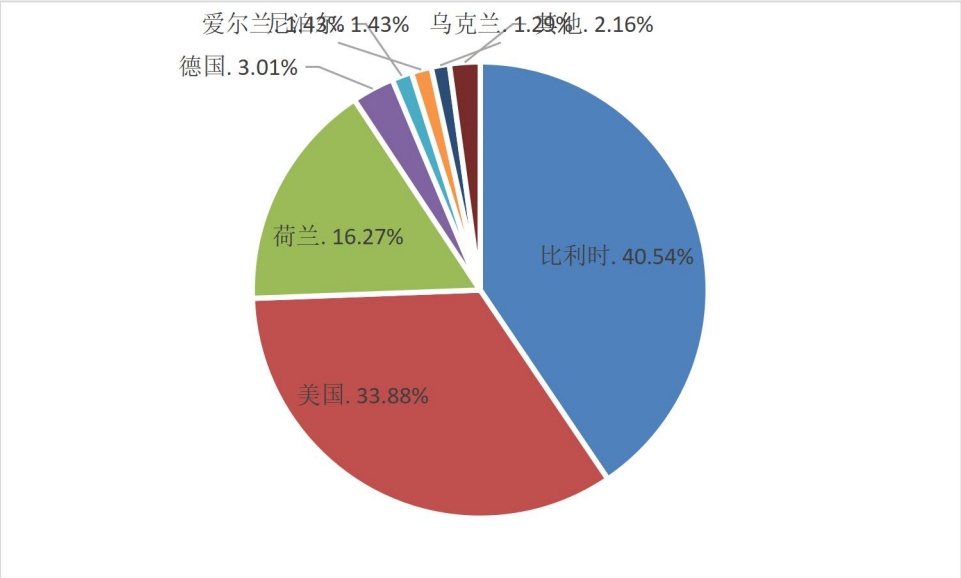

图 3 境外网络攻击分布及占比

（四）产品漏洞导致互联网安全风险

11 月份，通过对我省煤炭能源、钢铁冶金、电力行业企业网络通信行为分析研判，结合第三方威胁情报库比对，累计监测到符合漏洞利用特征的异常行为告警共 1119 次，涉及 13 家相关企业。从被利用漏洞类型来看，主要以远程控制、代码注入、信息读取等漏洞为主，其中高危漏洞 6 个（占比 75.00%）、中危漏洞 2 个（占比 25.00%）。

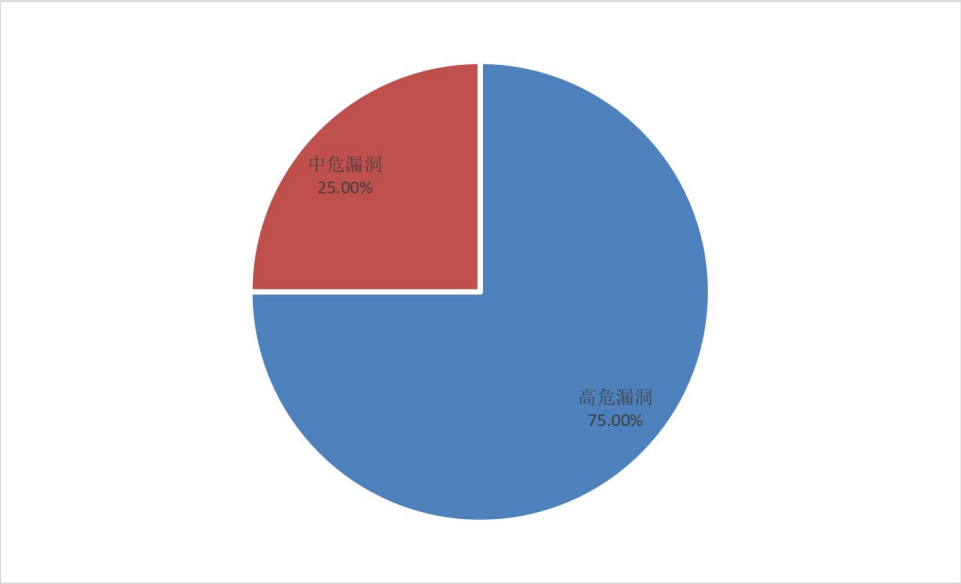

图 4 漏洞危害级别分布及占比

（五）挖矿木马感染持续发酵

11 月份，通过对我省煤炭能源、钢铁冶金、电力行业企业网络通信行为特征分析研判，结合第三方威胁情报库比对，累计触发挖矿木马行为特征相关网络告警 1437 次，涉及 8 家企业共 8 个互联网主机 IP，环比下降 63.64%（互联网主机 IP 环比下降 68.00%）。从挖矿木马家族来看，以 CoinMiner、BitMine、CoinHive 为主，其中 CoinMiner 家族最为活跃，门罗币为热门挖矿币种，主要的矿池服务 IP 为 139.177.196.162（加拿大）。

序号	木马家族	MD5 值	矿池 IP
1	CoinMiner	1bc841a2bf4eae4a0dee2f016943f336	139.177.196.162
2	BitMine	2cce1f2bd9a8d2b62179343cb497c64f	141.95.206.77
3	CoinHive	8350ba5e421b6034df13f2ba10329300	95.168.216.7

表 1 活跃挖矿木马家族 TOP3 详情

二、网络攻击态势

（一）网络攻击类型多样化

11 月份，通过提取网络攻击行为的特征分析研判发现，我省煤炭能源、钢铁冶金、电力等行业主要遭受网络攻击手

段包括但不限于：木马病毒感染（6264 次）、蠕虫病毒感染（5940 次）、网络扫描探测（2532 次）、漏洞利用尝试（1119 次）、僵尸网络感染（1067 次）、WEB 攻击尝试（477 次）等，其中木马病毒感染、蠕虫病毒感染、僵尸网络感染仍为主要网络攻击类型。

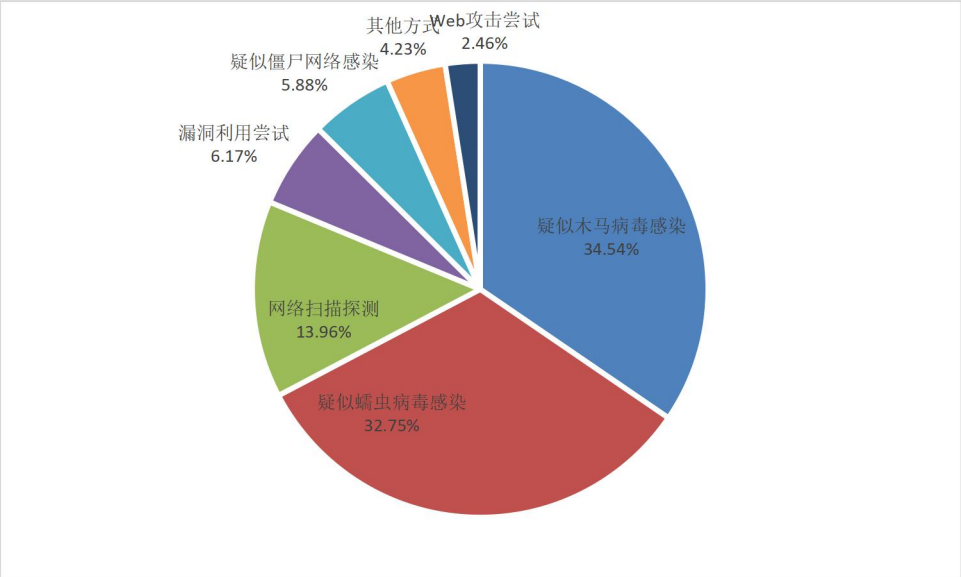

图 5 网络攻击告警分类及占比

（二）以漏洞利用为主的网络攻击突出

从漏洞利用攻击来分析，被利用的漏洞涉及组态软件、应用软件等，呈现多样化和高危等特征。其中以 Apache Log4j 远程代码执行漏洞（CVE-2021-44228）、PHPunit 远程代码执行漏洞（CVE-2017-9841）、Dasan GPON 路由器远程命令执行漏洞（CVE-2018-10562）、泛微 e-office 存在文件上传漏洞（CNVD-2021-49104）等高中危漏洞为主。

序号	漏洞编号	漏洞名称	危害级别	备注
1	CVE-2021-44228	Apache Log4j 远程代码执行漏洞	高危	
2	CVE-2017-9841	PHPunit 远程代码执行漏洞	高危	
3	CVE-2018-10562	Dasan GPON 路由器远程命令执行漏洞	高危	
4	CNVD-2021-49104	泛微 e-office 存在文件上传漏洞	高危	
5	CVE-2019-9670	Zimbra 远程代码执行漏洞	高危	

表 2 被利用漏洞 TOP5

从漏洞类型来看，web 应用漏洞 3 个、应用程序漏洞 3 个、网络设备漏洞 2 个。

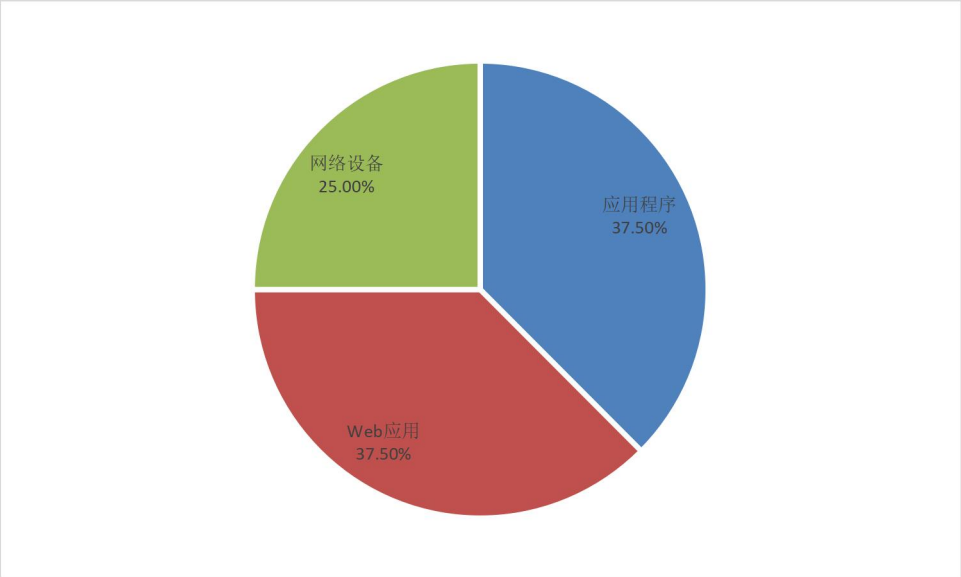

图 6 漏洞类型分布及占比

（三）Web 应用系统网络威胁不容忽视

11 月份，通过提取网络攻击行为的特征分析研判发现，针对工业企业 Web 应用系统（如门户网站、OA 系统等）的攻击，累计触发网络威胁告警 447 次。攻击手段包括文件上传绕过、远程控制命令、SQL 注入、XSS 攻击等。

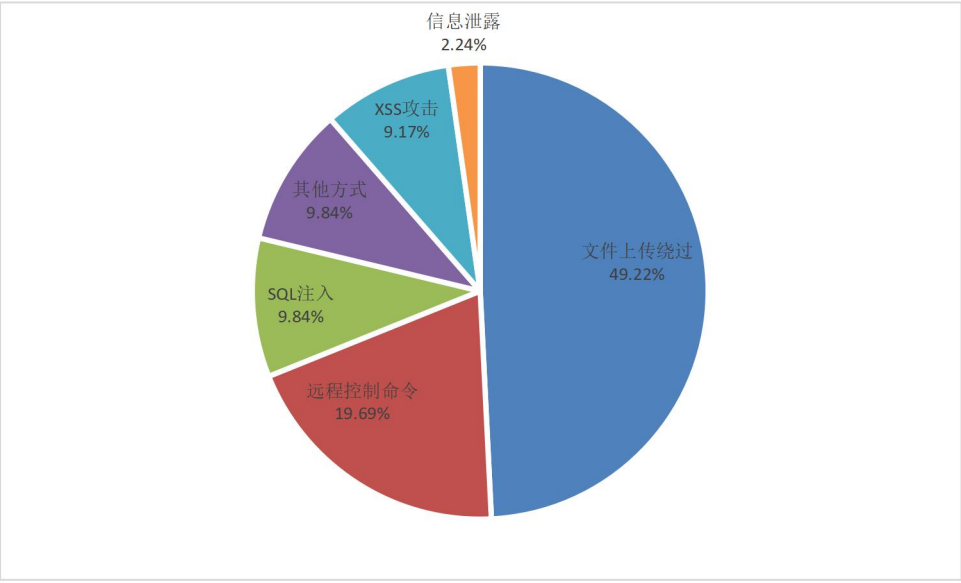

图 7 Web 攻击分类及占比

检测发现符合 SQL 注入特征的网络攻击 40 次，涉及 5 家企业 6 个互联网主机 IP，遭受攻击的主体包括致远 OA 系统、用友 U8 系统及以 ThinkPHP 为框架的系统等。

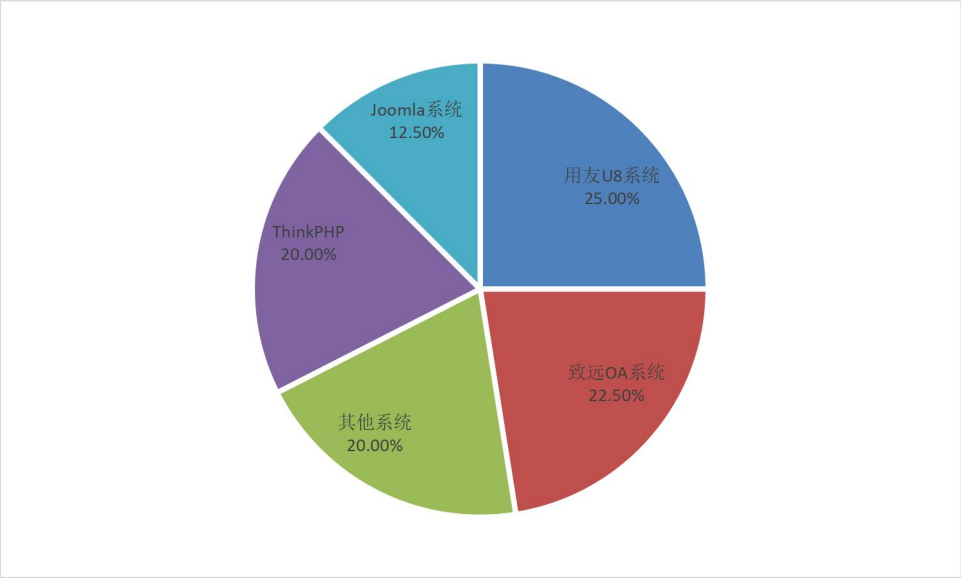

图 8 SQL 注入漏洞攻击对象及占比

三、行业安全态势

（一）煤炭能源行业主要威胁为僵木蠕感染

11 月份，监测发现省内煤炭能源行业共 50 家企业 69 个互联网主机 IP 遭受网络攻击，累计触发网络威胁告警 13762 条，占本月行业监测威胁告警总数的 75.88%。

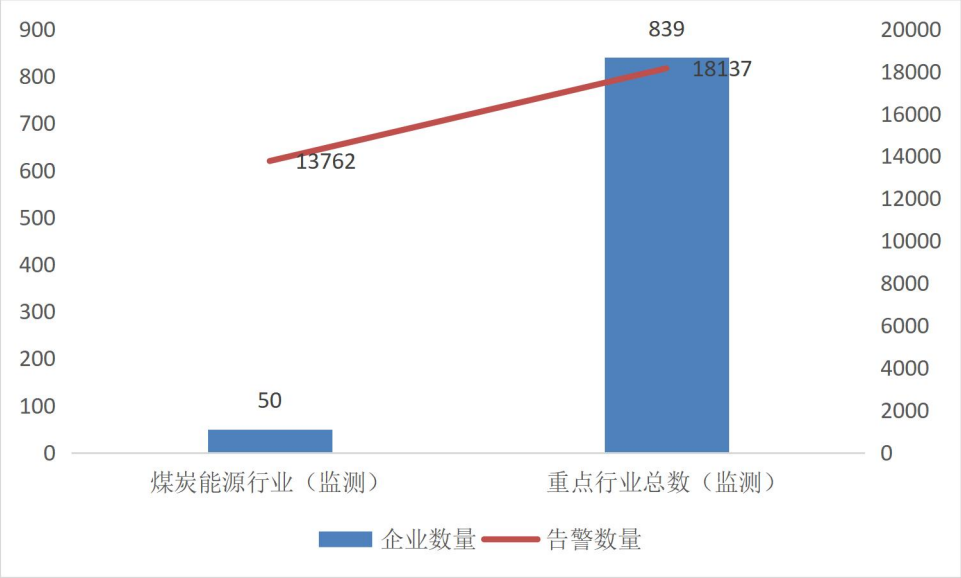

图 9 煤炭行业遭受攻击企业数量及次数

针对煤炭行业的网络攻击手段主要类型包含僵木蠕病毒感染、漏洞利用尝试及 Web 攻击尝试等，主要以蠕虫病毒、木马病毒、僵尸网络感染等为主，占比分别为 43.10%、35.33%、6.54%，合计占行业网络威胁总数的 84.97%，是当前该行业网络侧面临的主要安全威胁。

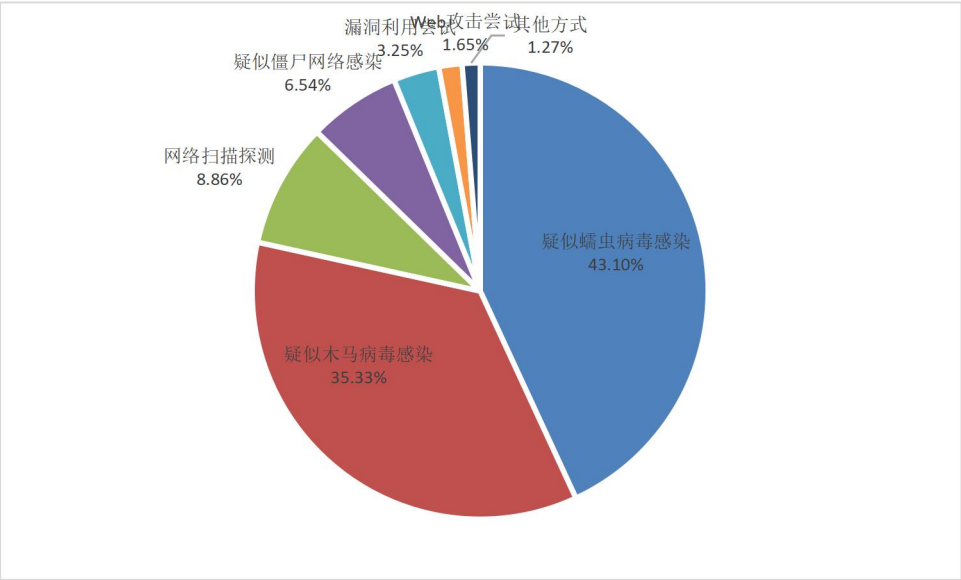

图 10 煤炭能源行业遭受网络攻击类型分布及占比

（二）钢铁冶金行业频繁遭受恶意嗅探

11 月份，监测发现省内钢铁冶金行业遭受网络攻击达 2823 次，主要的攻击手段主要类型为网络嗅探（1293 次），包括以扫描探测、登录尝试等常用的信息收集，其中扫描探测为 1158 次，占比 89.56%，登录尝试 85 次，占比 6.57%。

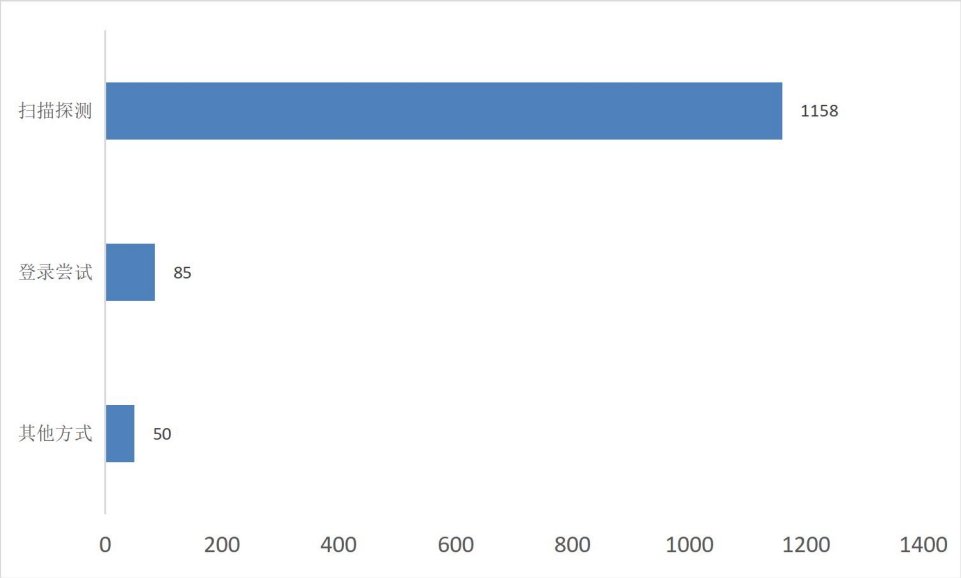

图 11 钢铁冶金行业遭受网络攻击类型及数量

从网络嗅探的扫描器种类分析，主要以 Zgrabe、Nmap、Masscan 等黑客常用扫描工具为主。

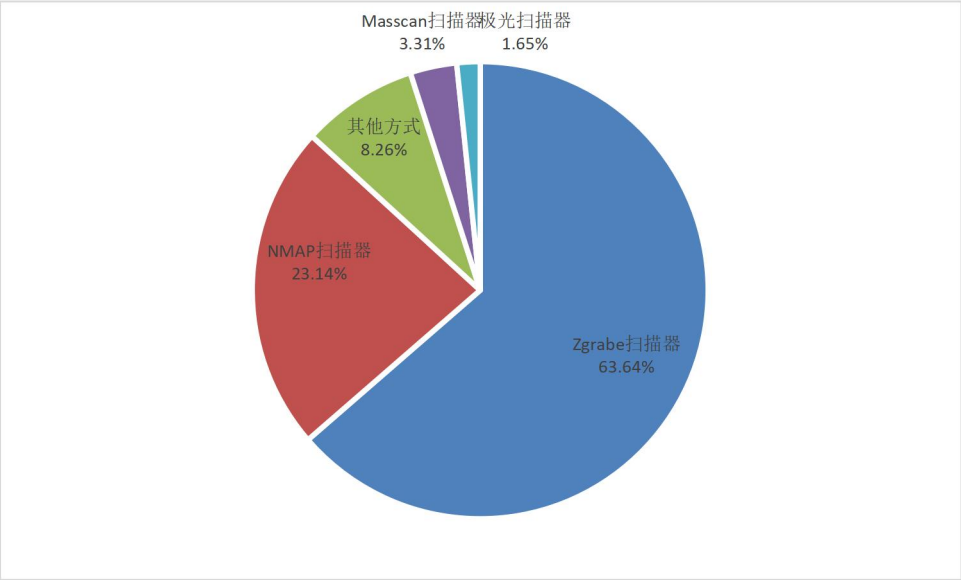

图 12 钢铁冶金行业遭受网络嗅探分类及占比

（三）电力行业遭受网络攻击主要来自境外

11 月份，监测发现省内电力行业遭受网络攻击 1552 次，涉及的 11 家企业 15 个互联网主机 IP，攻击手段包括木马后门通信、系统渗透等。

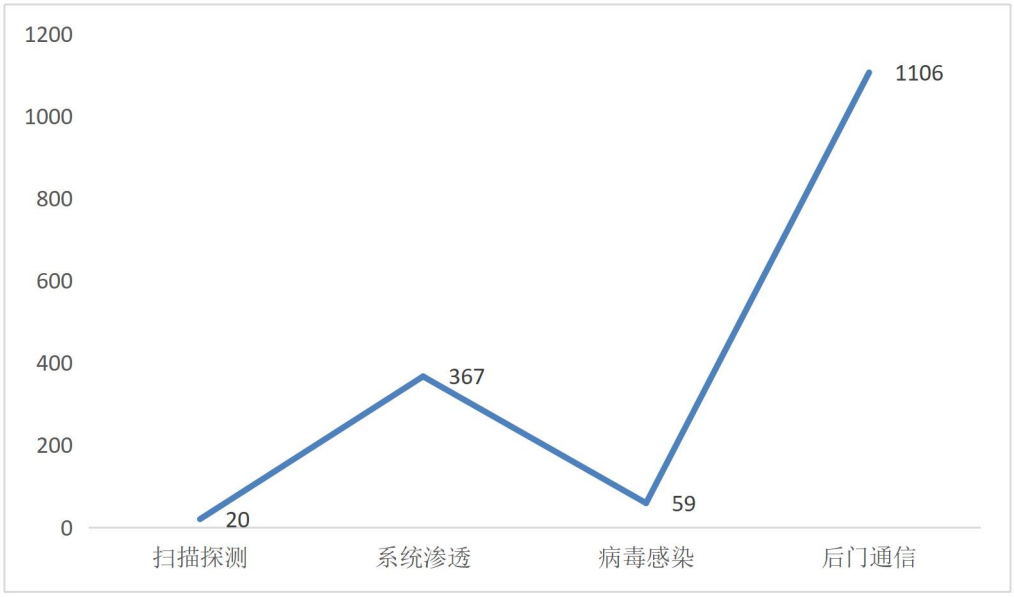

图 13 电力行业遭受网络攻击类型及数量

通过对电力行业网络威胁告警分析研判，结合第三方威胁情报库比对，针对本行业的网络攻击、远程命令和控制服务器多数位于境外，合计占比超七成，其中来自荷兰的网络攻击数量最多，达 756 次，占电力行业本月网络威胁告警总数的 48.71%。

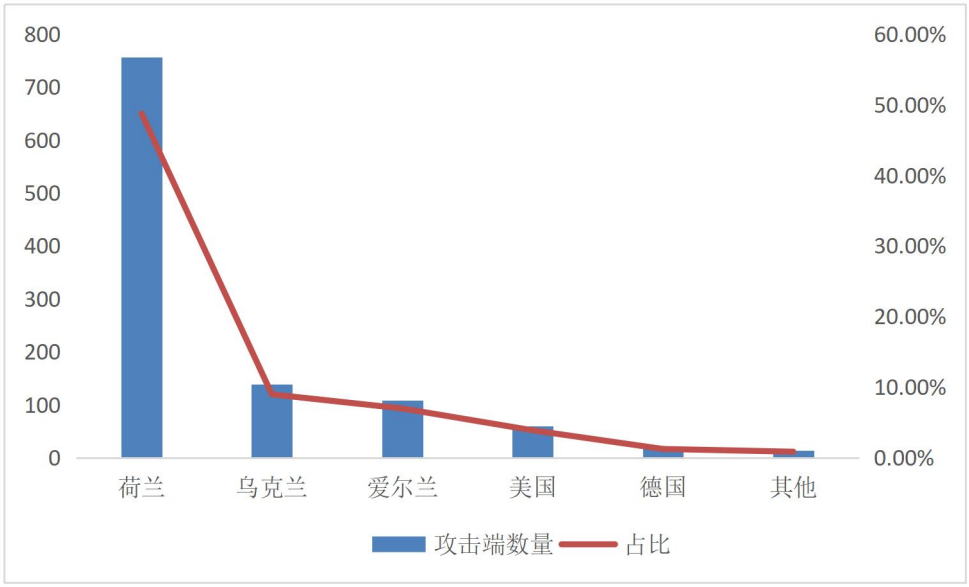

图 14 电力行业遭受网络攻击归属分布

四、网络安全预警提示

煤炭能源、钢铁冶金、电力行业在我省属于重要基础性行业，一旦发生大规模网络安全事件，对我省经济社会将产生严重影响。随着互联网技术、物联网技术的深入广泛应用，网络攻击面持续扩大，相关行业面临的网络安全威胁和挑战不容忽视。

针对公共互联网的安全防护，一方面要提升企业网络安全意识和技术防护能力，应依据《网络安全法》等法律法规，严格落实网络安全主体责任，加大网络安全投入，规范产品安全功能要求，定期开展网络安全检查和评估，加强网络安全培训，提高企业各层级网络安全防护意识；另一方面要加强行业、企业和用户对自身网络资产梳理和检查，进一步做好安全防范措施，建立产品安全漏洞发现、修复机制，定期开展网络安全漏洞扫描，更新漏洞补丁，及时对不常用的服务端口采取关闭或加固措施，强化风险闭环管控，并做好重

要数据备份；要加快网络安全技术手段建设，提升网络流量分析能力，细化流量分析粒度，不断提高技术防范能力。

附录

11 月被利用漏洞及频次

序号	漏洞编号	漏洞名称	危害级别	频次
1	CVE-2021-44228	Apache Log4j 远程代码执行漏洞	高危	31
2	CVE-2017-9841	PHPunit 远程代码执行漏洞	高危	5
3	CVE-2018-10562	Dasan GPON 路由器远程命令执行漏洞	高危	4
4	CNVD-2021-49104	泛微 e-office 存在文件上传漏洞	高危	3
5	CVE-2019-9670	Zimbra 远程代码执行漏洞	高危	2
6	CVE-2019-16920	D-Link 路由器远程命令执行漏洞	高危	2
7	CVE-2021-21402	Jellyfin 任意文件读取漏洞	中危	2
8	CVE-2021-41773	Apache HTTP Server 路径遍历漏洞	中危	1

建议相关行业企业重点排查高频次被利用漏洞，及时从官方网站获取漏洞详情，并采取修复措施，防止发生网络安全事件。

信息编辑：山西省通信管理局
网络安全管理处

技术支撑：山西省信息通信网络技术
保障中心

地址：太原市南内环街 2 号