山西省
煤炭能源、钢铁冶金、电力行业
10月份网络安全态势分析

2022年12月

10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

10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77家企业（127个互联网主机）疑似遭受网络攻击（其中煤炭能源55家企业94台互联网主机，钢铁冶金8家企业15台互联网主机，电力行业14家企业18台互联网主机），累计触发相关网络威胁告警62673条，网络威胁告警呈上升趋势，其中作为被攻击方遭受恶意网络攻击触发威胁告警58394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4679次。

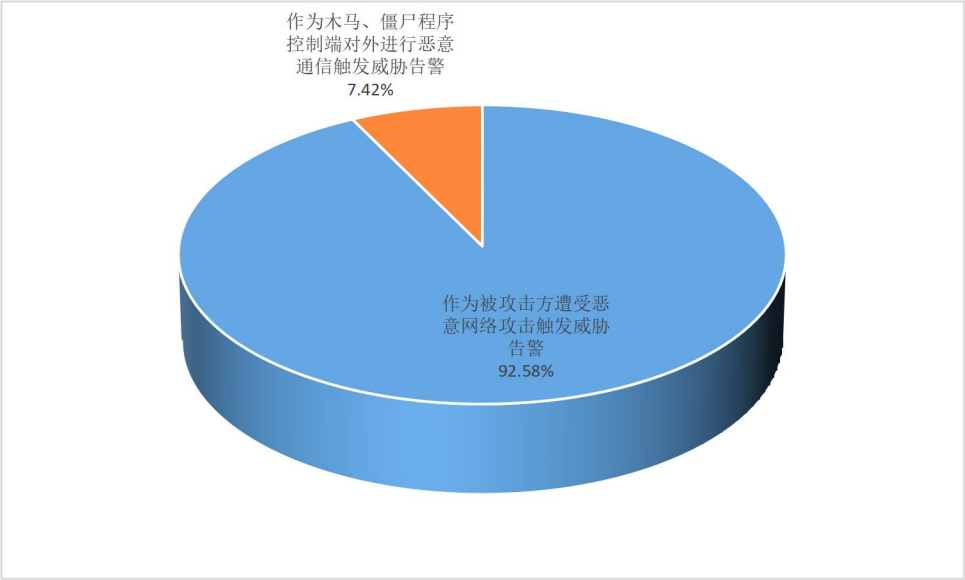

图 1 触发相关网络威胁告警分布及占比

（二）恶意网络资源是面临的主要威胁

10 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，发现 29 台互联网主机频繁访问恶意域名和恶意 IP，累计触发网络威胁告警 33700 余次，其中被访问的恶意网络资源（恶意域名和恶意 IP） 主要包含: fget-career.com、*.jifr.*、*.beahh.com 等。

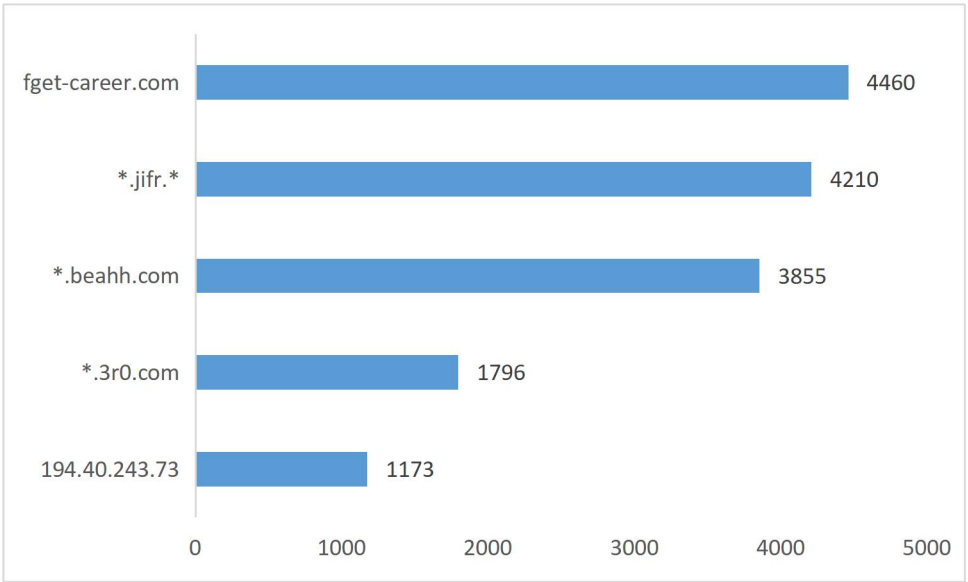

图 2 恶意域名和恶意 IPTOP5

（三）挖矿木马感染持续发酵

10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5488次，涉及22家企业共25台互联网主机IP。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194.40.243.73（乌克兰）。

序号	木马家族	MD5值	矿池IP
1	CoinMiner	df89c542407b47b5ca50095fd04ad5e1	194.40.243.73
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

10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、电力行业主要遭受网络攻击手段包括但不限于：木马病毒感染（27501次）、蠕虫病毒感染（12766次）、僵尸网络感染（9952次）、网络扫描探测（6901次）、漏洞利用尝试（927次）、WEB攻击尝试（822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。

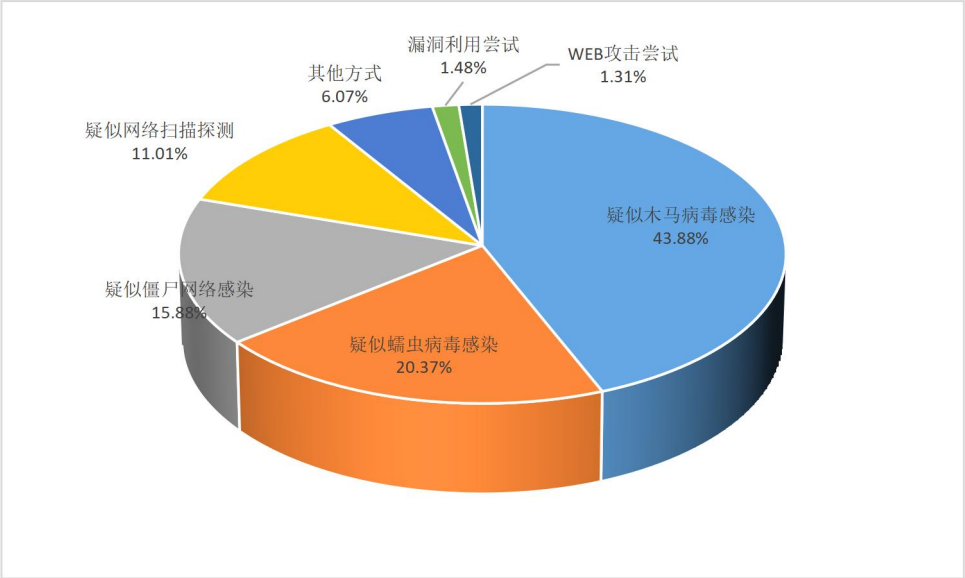

图 3 网络攻击告警分类及占比

（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）、Bash 远程代码执行漏洞（CVE-2014-6271）、D-link DCS 2530L 和 DCS 2670L 监控信息泄露漏洞（CVE-2020-25078）、PHPunit 远程代码执行漏洞（CVE-2017-9841）、Apache HTTP Server 路径遍历漏洞（CVE-2021-41773）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-2014-6271	Bash 远程代码执行漏洞	高危	
3	CVE-2020-25078	D-link DCS 2530L 和 DCS 2670L 监控信息泄露漏洞	中危	
4	CVE-2017-9841	PHPunit 远程代码执行漏洞	高危	
5	CVE-2021-41773	Apache HTTP Server 路径遍历漏洞	中危	

表 2 被利用漏洞 TOP5

（三）互联网应用产品漏洞的高危害级别占比突出

10 月份，通过匹配网络攻击行为中漏洞利用特征分析研判，累计监测触发符合漏洞利用特征的异常行为告警共 987

次，涉及 21 家重点企业。从被利用漏洞类型来看，主要以信息读取、代码注入、远程控制等漏洞为主，其中高危漏洞 35 个（占比 72.92%）、中危漏洞 11 个（占比 25.00%）、低危漏洞 1 个（占比 2.08%）。

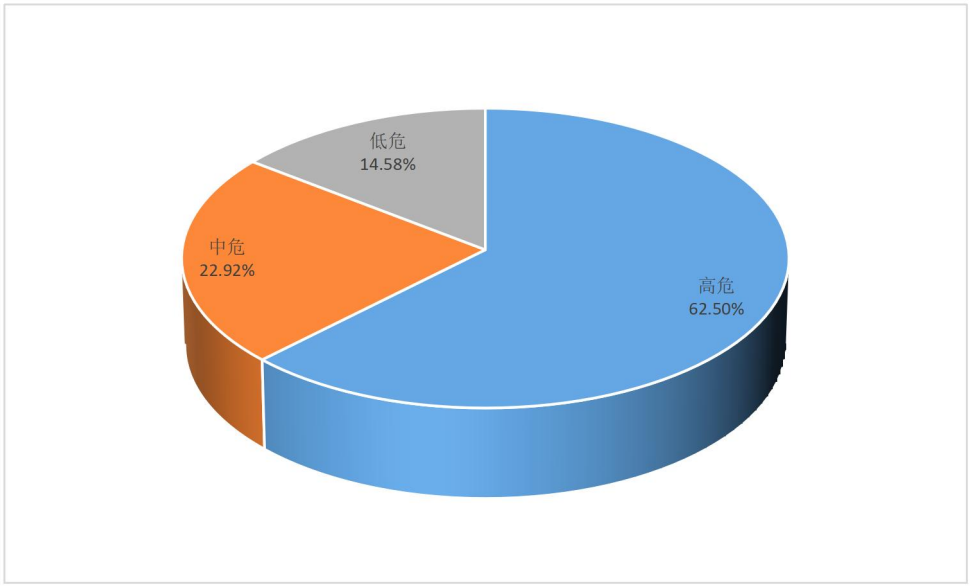

图 4 漏洞危害级别分布及占比

从漏洞类型来看，web 应用漏洞 18 个、应用程序漏洞 17 个、网络设备漏洞 7 个、操作系统漏洞 5 个、数据库漏洞 1 个。

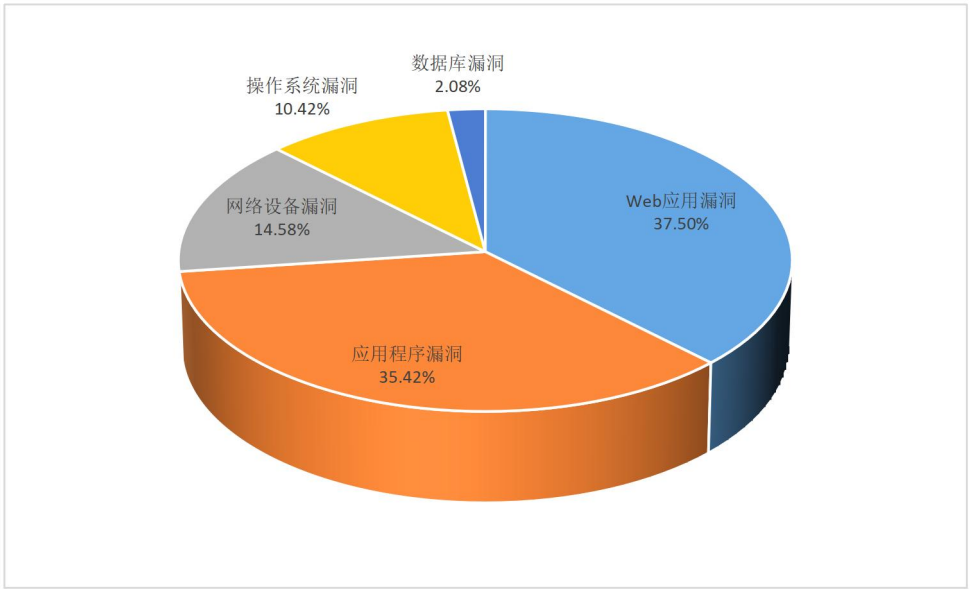

图 5 漏洞类型分布及占比

三、行业遭受网络攻击情况

（一）煤炭能源行业主要威胁为僵木蠕感染

10 月份，监测发现省内煤炭能源行业遭受网络攻击的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，主要以木马病毒、蠕虫病毒、僵尸网络感染等为主，占比分别为 34.58%、27.36%、11.90%，合计占行业网络威胁总数的 73.84%，是当前该行业网络侧面临的主要安全威胁。

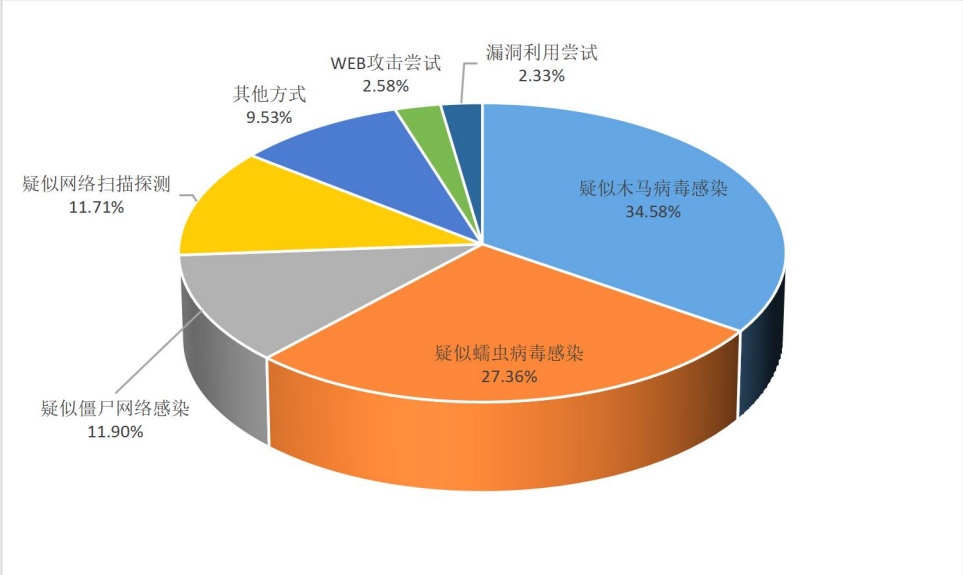

图 6 煤炭能源行业遭受网络攻击类型分布及占比

（二）钢铁冶金行业频繁遭受恶意嗅探

10 月份，监测发现省内钢铁冶金行业遭受网络攻击的主要类型为网络嗅探，达 3947 次，主要以扫描探测、登录尝试等常用的信息收集手段为主，其中扫描探测为 3700 次，占比 93.74%，登录尝试 220 次，占比 5.57%。

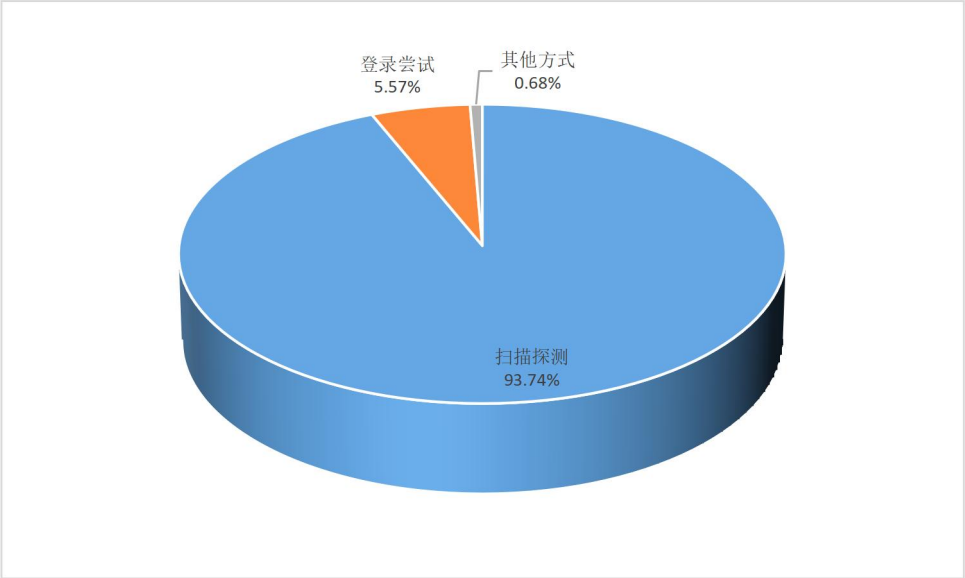

图 7 钢铁冶金行业遭受网络攻击类型分布及占比

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

10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	470
2	CVE-2014-6271	Bash 远程代码执行漏洞	高危	181
3	CVE-2020-25078	D-link DCS 2530L 和 DCS 2670L 监控信息泄露漏洞	中危	42
4	CVE-2017-9841	PHPunit 远程代码执行漏洞	高危	37
5	CVE-2021-41773	Apache HTTP Server 路径遍历漏洞	中危	29
6	CVE-2020-26217	XStream 反序列化远程代码执行漏洞	高危	20
7	CNVD-2018-04757	帆软 FineReport 8.0 版本任意文件读取漏洞	中危	19
8	CVE-2020-9054	合勤 ZyXEL 网络存储器(NAS)设备远程代码执行漏洞	高危	18
9	CVE-2017-15718	Hadoop YARN NodeManager 密码泄露漏洞	中危	17
10	CVE-2018-10562	Dasan GPON 路由器远程命令执行漏洞	高危	16
11	CNVD-2021-01627	致远 OA 系统存在文件上传漏洞	高危	14
12	CVE-2020-15227	Nette 框架远程代码执行漏洞	高危	14
13	CVE-2019-2725	WebLogic 反序列化远程命令执行漏洞	高危	10
14	CVE-2012-1823	PHP-CGI 远程任意代码执行漏洞	高危	8
15	CVE-2021-40870	Aviatrix Controller 远程代码执行漏洞	高危	8
16	CVE-2019-9670	Zimbra 远程代码执行漏洞	高危	7
17	CVE-2019-16920	D-Link 路由器远程命令执行漏洞	高危	6
18	CVE-2021-26084	Confluence 远程代码执行漏洞	高危	6
19	CVE-2017-10271	Oracle WebLogic Server WebLogic WLS 组件远程命令执行漏洞	高危	5
20	CVE-2018-13379	Fortinet FortiOS 路径遍历漏洞	中危	5
21	CVE-2017-5638	Struts2(S2-045)远程代码执行漏洞	高危	4
22	CVE-2020-5410	VMware Spring Cloud Config 路径遍历漏洞	中危	4
23	CNVD-2021-45203	TamronOS IPTV/VOD 系统存在命令执行漏洞	高危	3
24	CVE-2019-11510	Pulse Secure Pulse Connect Secure 任意文件读取漏洞	高危	3
25	CVE-2019-12725	Zeroshell 远程命令执行漏洞	高危	3
26	CVE-2019-7238	Nexus Repository Manager 3 远程代码执行漏洞	高危	3
27	CVE-2020-15568	TerraMaster TOS 动态类方法调用漏洞	高危	3
28	CVE-2021-21402	Jellyfin 任意文件读取漏洞	中危	3
29	CNVD-2021-49104	泛微 e-office 存在文件上传漏洞	高危	2
30	CVE-2015-8399	Atlassian Confluence 信息泄露漏洞	中危	2

31	CVE-2016-3081	Apache Struts2 远程代码执行漏洞	高危	2
32	CVE-2017-11610	Supervisor 远程命令执行漏洞	高危	2
33	CVE-2019-14470	WordPress UserPro 插件跨站脚本漏洞	中危	2
34	CVE-2019-16759	vBulletin 远程命令执行漏洞	高危	2
35	CVE-2019-17506	D-Link DIR-817LW 和 D-Link DIR-868L 授权问题漏洞	高危	2
36	CVE-2019-3396	Atlassian Confluence Server 服务器端模板注入漏洞	高危	2
37	CVE-2020-10199	Sonatype Nexus Repository Manager 命令执行漏洞	高危	2
38	CVE-2007-4556	XWork AltSyntax 功能 OGNL 命令注入漏洞	高危	1
39	CVE-2013-4212	Apache Roller OGNL 表达式注入远程代码执行漏洞	高危	1
40	CVE-2018-1000533	Gitist 0.6.0 远程命令执行漏洞	高危	1
41	CVE-2019-3929	多款无线演示系统存在未授权远程命令执行漏洞	高危	1
42	CVE-2020-28188	TerraMaster TOS 远程命令执行漏洞	高危	1
43	CVE-2020-3452	Cisco ASA 系列任意文件读取漏洞	中危	1
44	CVE-2020-8515	DrayTek Vigor 系列任意命令执行漏洞	低危	1
45	CVE-2020-9484	ApacheTomcat 代码问题漏洞	中危	1
46	CVE-2021-32305	WebSVN 命令注入漏洞	高危	1
47	CVE-2021-36749	Apache Druid LoadData 存在任意文件读取漏洞	中危	1
48	CVE-2021-42013	Apache HTTP Server 目录遍历漏洞	高危	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

电话/传真：0351-8788110