中国地质大学（武汉）校园网络安全年报

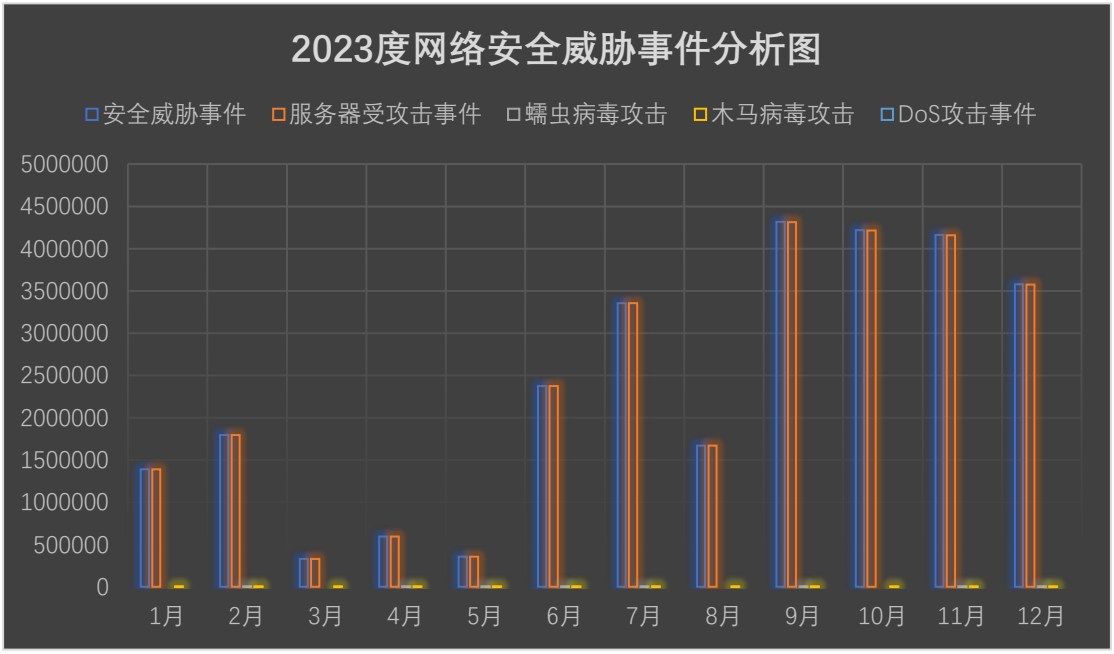
2023 年度

中国地质大学（武汉）信息化工作办公室　　2023 年 1 月-2023 年 12 月

1、情况综述

2023 年学校总体网络安全情况良好，未发生重大的网络安全事件。

根据监测分析，2023 年校园网络发生的安全威胁事件 28134059 起、服务器受攻击威胁事件 28120034 起、蠕虫病毒攻击 545 起、木马病毒攻击 13480 起、DoS 攻击 0 起。



2023 度安全监测数据统计表

时间	安全威胁事件	服务器受攻击事件	确认僵尸主机	DoS 攻击事件	黑链攻击
1 月	1391276	1390676	0	600	0
2 月	1793840	1793164	88	588	0

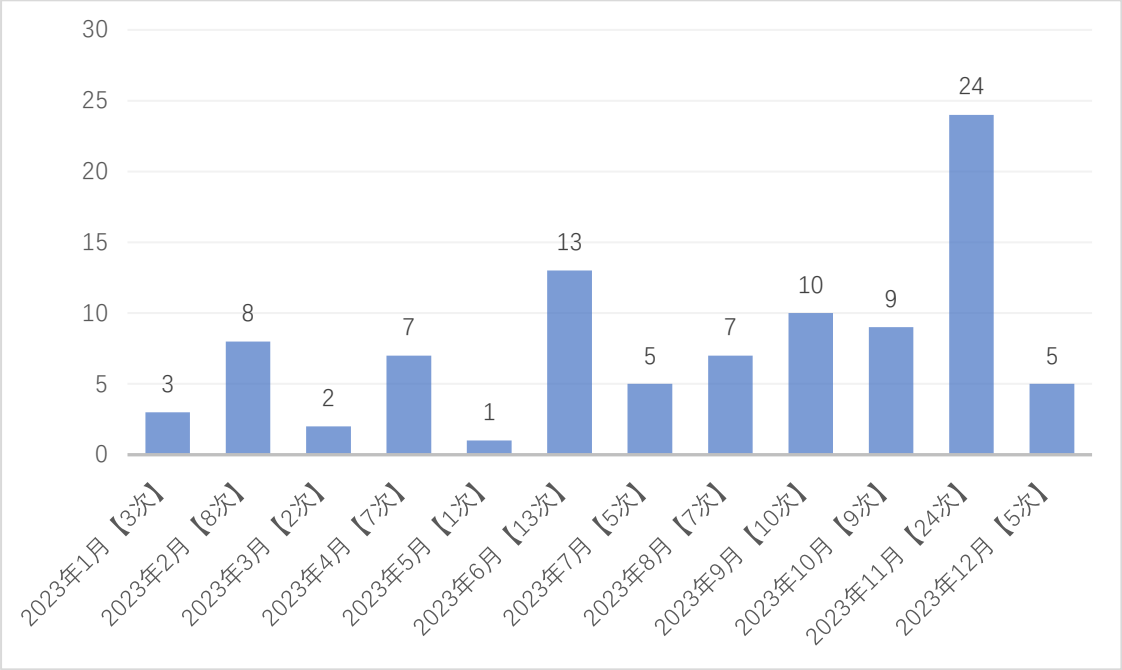
3 月	328425	328299	0	126	0
4 月	594180	593977	11	192	0
5 月	356277	356195	10	72	0
6 月	2374920	2372951	248	1721	0
7 月	3354299	3353184	3	1112	0
8 月	1670951	1669602	0	1349	0
9 月	4315891	4312430	178	3283	0
10 月	4217107	4215578	1	1528	0
11 月	4160529	4159322	4	1203	0
12 月	3576364	3574656	2	1706	0

2、安全事件通报

2024 度信息化工作办公室共计处理网络安全通报事件共 94 起，分别为：教育系统网络安全工作管理平台安全监测预警子系统通报事件 30 教育行业网络安全平台通报事件 29 起，湖北省网络与信息安全信息通报中心通报事件 4 起，学校自查事件 31 起。

具体内容如下：

2023 度网络安全事件通报分析图



2023 度网络安全事件汇总表

时间	通报日期	通报单位	内容	处理结果
1 月	1 月 4 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在应用框架漏洞问题	已整改
	1 月 10 日	学校内部自查	某网站存在外链问题	已整改
	1 月 18 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在信息泄露问题	已整改
2 月	2 月 7 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	2 月 7 日	教育部漏洞报告平台	某信息系统存在配置及设计漏洞问题	已整改
	2 月 7 日	教育部漏洞报告平台	某信息系统存在未授权访问、敏感信息泄露问题	已整改
	2 月 7 日	教育部漏洞报告平台	某信息系统存在注入问题	已整改
	2 月 8 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在信息泄露问题	已整改
	2 月 9 日	教育部漏洞报告平台	某信息系统存在信息泄露问题	已整改
	2 月 16 日	教育部漏洞报告平台	某信息系统存在弱口令、设计漏洞问题	已整改

时间	通报日期	通报单位	内容	处理结果
	2 月 16 日	教育部漏洞报告平台	某信息系统配置失效漏洞问题	已整改
3 月	3 月 21 日	教育部漏洞报告平台	某信息系统存在系统软件设计漏洞问题	已整改
	3 月 21 日	教育部漏洞报告平台	某信息系统存在弱口令问题	已整改
4 月	4 月 6 日	学校内部自查	某网站存在敏感信息泄露问题	已整改
	4 月 6 日	学校内部自查	某网站存在敏感信息泄露问题	已整改
	4 月 8 日	学校内部自查	某信息系统存在暗链问题	已整改
	4 月 8 日	学校内部自查	某网站存在暗链问题	已整改
	4 月 21 日	教育部漏洞报告平台	某信息系统存在弱口令、系统设计问题	已整改
	4 月 24 日	学校内部自查	某网站存在敏感信息泄露问题	已整改
	4 月 27 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
5 月	5 月 17 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
6 月	6 月 5 日	学校内部自查	某信息系统存在弱口令问题	已整改
	6 月 5 日	学校内部自查	某信息系统存在弱口令问题	已整改
	6 月 5 日	学校内部自查	某信息系统存在弱口令问题	已整改
	6 月 5 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在远程命令执行漏洞问题	已整改
	6 月 6 日	教育部漏洞报告平台	某信息系统存在弱口令、数据库命令执行漏洞问题	已整改
	6 月 6 日	教育部漏洞报告平台	某信息系统存在弱口令问题	已整改
	6 月 6 日	教育部漏洞报告平台	某信息系统存在弱口令问题	已整改
	6 月 6 日	教育部漏洞报告平台	某信息系统存在弱口令问题	已整改
	6 月 6 日	教育部漏洞报告平台	某信息系统存在弱口令、XSS 跨站脚本漏洞问题	已整改
	6 月 6 日	教育部漏洞报告平台	某信息系统存在暗链问题	已整改
	6 月 8 日	教育部漏洞报告平台	某信息系统存在越权漏洞、敏感信息枚举问题	已整改
	6 月 9 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	6 月 27 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在信息泄露问题	已整改
7 月	7 月 10 日	教育部漏洞报告平台	某信息系统存在信息泄露问题	已整改
	7 月 10 日	教育部漏洞报告平台	某信息系统存在信息泄露问题	已整改
	7 月 10 日	教育部漏洞报告平台	某信息系统存在双非、系统软	已整改

时间	通报日期	通报单位	内容	处理结果
			件设计漏洞问题	
	7 月 18 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在访问控制及系统配置失效问题	已整改
	7 月 22 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在信息泄露问题	已整改
8 月	8 月 13 日	教育部漏洞报告平台	某小程序存在逻辑漏洞问题	已整改
	8 月 28 日	教育系统网络安全工作管理平台安全监测预警子系统	某主机存在 Ramnit 蠕虫病毒问题	已整改
	8 月 28 日	教育部漏洞报告平台	某信息系统存在信息泄露问题	已整改
	8 月 30 日	学校内部自查	某信息系统存在敏感配置文件泄露问题	已整改
	8 月 30 日	学校内部自查	某网站存在敏感信息泄露问题	已整改
	8 月 31 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在未授权访问问题	已整改
	8 月 31 日	教育部漏洞报告平台	某信息系统存在弱口令问题	已整改
9 月	9 月 1 日	教育系统网络安全工作管理平台安全监测预警子系统	某信息系统存在信息泄露问题	已整改
	9 月 1 日	教育部漏洞报告平台	某信息系统存在双非、逻辑漏洞问题	已整改
	9 月 1 日	教育部漏洞报告平台	某信息系统存在反序列化漏洞问题	已整改
	9 月 1 日	教育部漏洞报告平台	某信息系统存在逻辑漏洞问题	已整改
	9 月 1 日	教育部漏洞报告平台	某信息系统存在缓冲区溢出漏洞问题	已整改
	9 月 5 日	教育部漏洞报告平台	某信息系统存在弱口令问题	已整改
	9 月 18 日	湖北省网络与信息安全信息通报中心	某邮箱疑似被发送钓鱼邮件	已整改
	9 月 18 日	湖北省网络与信息安全信息通报中心	某信息系统存在任意文件读取问题	已整改
	9 月 18 日	湖北省网络与信息安全信息通报中心	某信息系统存在任意文件读取问题	已整改
	9 月 19 日	教育部漏洞报告平台	某信息系统存在任意用户登录、敏感信息泄漏问题	已整改
10 月	10 月 8 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	10 月 8 日	教育部漏洞报告平台	某信息系统存在双非问题	已整改

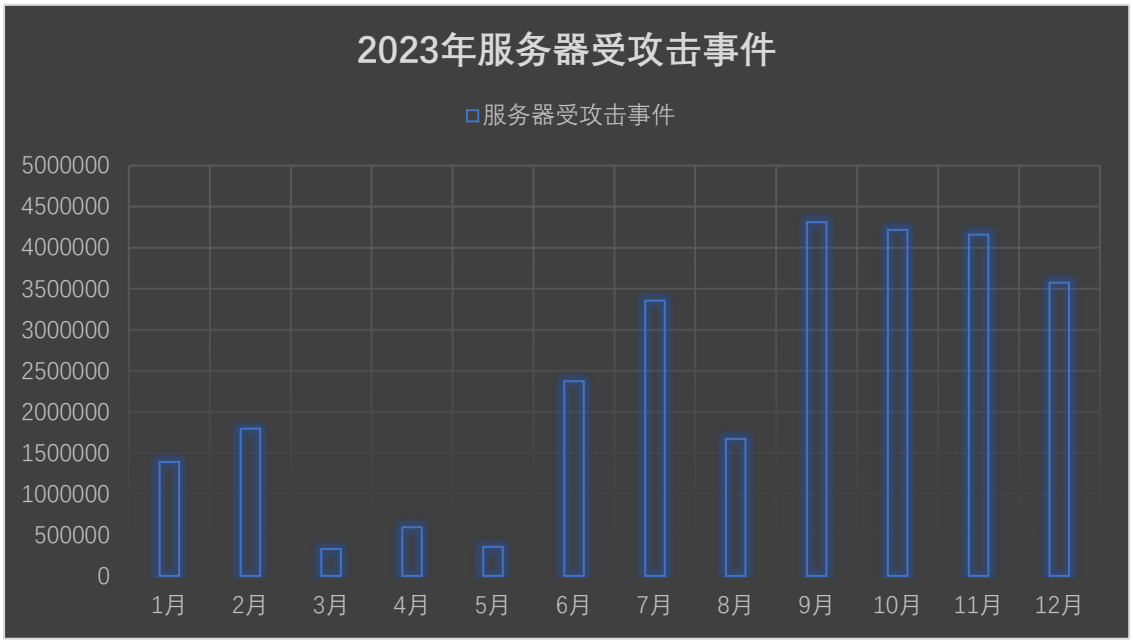
时间	通报日期	通报单位	内容	处理结果
	10 月 10 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	10 月 18 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	10 月 18 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	10 月 20 日	学校内部自查	某信息系统存在 SQL 注入问题	已整改
	10 月 20 日	学校内部自查	某信息系统存在 XXE 漏洞、系统敏感文件读取等严重问题	已整改
	10 月 25 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	10 月 31 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
11 月	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	发某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 2 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 7 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 7 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 7 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 7 日	学校内部自查	某网站存在暗链问题	已整改
	11 月 7 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	11 月 13 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改

时间	通报日期	通报单位	内容	处理结果
	11 月 13 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在敏感信息泄露问题	已整改
	11 月 13 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	11 月 15 日	湖北省网络与信息安全信息通报中心	某网站存在越权漏洞问题	已整改
	11 月 16 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
12 月	12 月 5 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	12 月 21 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	12 月 21 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	12 月 21 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改
	12 月 21 日	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在暗链问题	已整改

3、服务器受攻击情况

2023 度学校服务器受攻击事件共 28120034 起，平均月攻击次数为 2343336 次，主要攻击类型为网站扫描、Web 网站系统漏洞、WEBSHELL 上传、缓冲区溢出检测、SQL 注入、信息泄漏攻击。

2023 度学校服务器受攻击明细图



2023 度学校服务器受攻击次数 TOP10 服务器列表

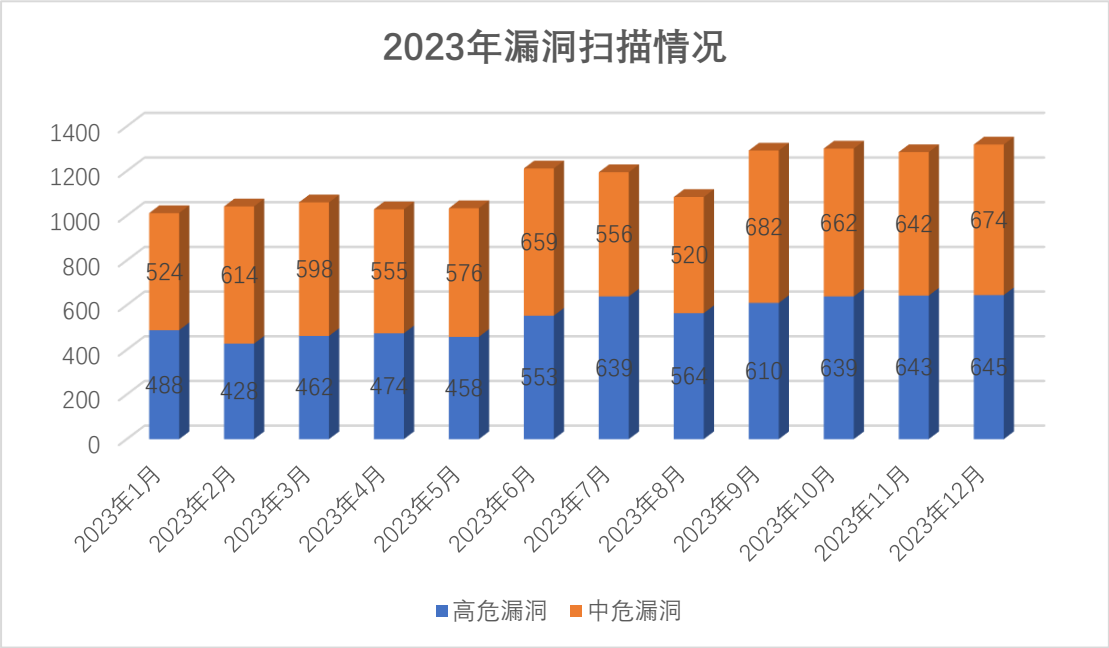
序号	目标服务器 IP/名称	攻击次数
1	校园虚拟专用（VPN）网络	3205539
2	站群系统	2125825
3	应用系统监测巡检系统	1653216
4	人事信息管理系统	543536
5	地球科学在线	538253
6	珠宝学院主页	260009
7	图书馆主页	214315
8	教室个人主页	199000
9	远程教学学习管理系统	182494
10	虚拟仿真平台	159074

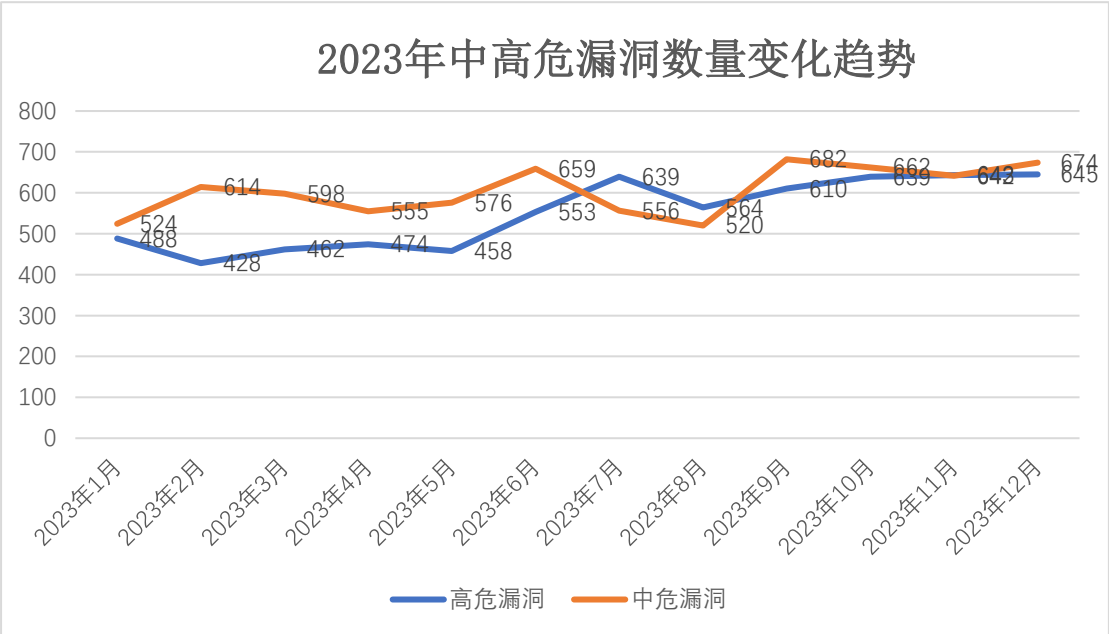
4、服务器漏洞扫描分析

2023 针对校园网服务器漏洞扫描检测工作成果如下：

2023 度针对 442 系统共完成定期扫描 24 次，现存风险漏洞 1319 高危风险

漏洞 645 个，高危风险漏洞 674 个。

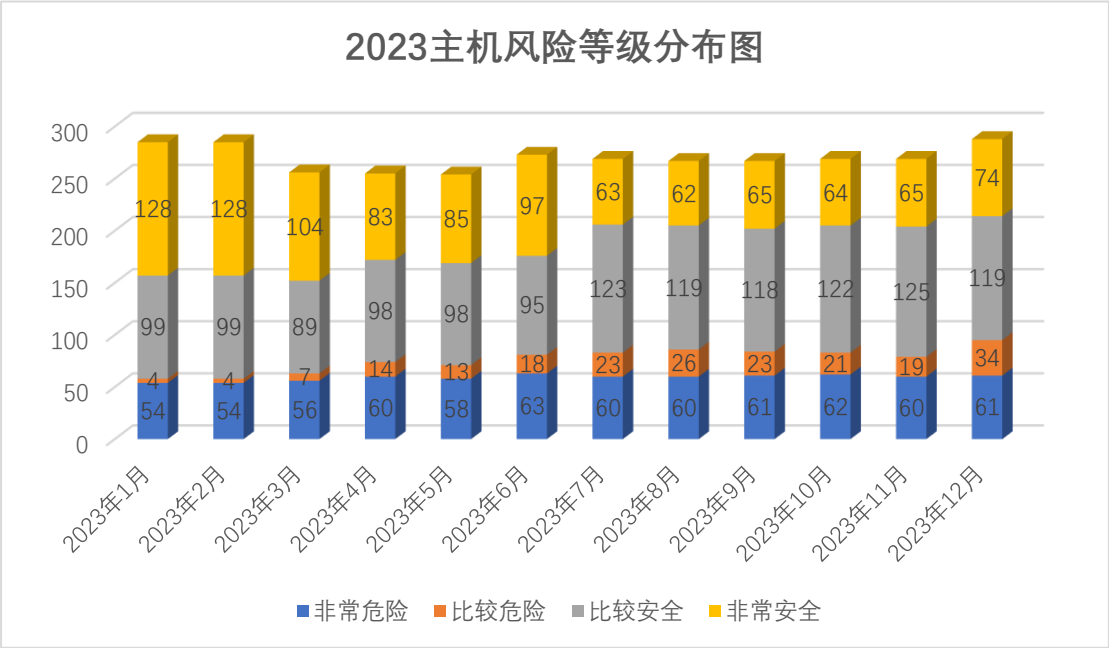




2023 年度主机风险等级分布表

时间	非常危险	比较危险	比较安全	非常安全	主机数
2023 年 1 月	54	4	99	128	285
2023 年 2 月	54	4	99	128	285
2023 年 3 月	56	7	89	104	256
2023 年 4 月	60	14	98	83	255
2023 年 5 月	58	13	98	85	254
2023 年 6 月	63	18	95	97	273

2023 年 7 月	60	23	123	63	269
2023 年 8 月	60	26	119	62	267
2023 年 9 月	61	23	118	65	267
2023 年 10 月	62	21	122	64	269
2023 年 11 月	60	19	125	65	269
2023 年 12 月	61	34	119	74	288



黑客攻击校园网络的主要方式为漏洞攻击。信息化工作办公室根据“策略放通，检测先行；逐月漏检、整改下发；认真执行、确保安全”的原则开展整改工作。通过每月进行的漏洞整改情况、漏洞检测报告的分析，结合防火墙策略控制手段，尽量将网络安全风险控制在局部，同时督促发现系统漏洞的单位按照信息化工作办公室给出的整改建议尽快完成漏洞整改工作。

5、安全漏洞整改情况

信息化工作办公室对扫描出来的安全漏洞给出了具体的整改建议。有重点分批次通知各服务器或应用系统所属部门系统管理员，按照漏洞危险程度逐步完成整改。2023 年度完成信息系统和网站漏洞扫描任务 121 次，复检 45 次，共下发系统整改通知书 265 份，邮件提醒督促漏洞整改工作 265 封。目前 80 余个系统完成漏洞整改，累计完成漏洞整改 1155 个，其中整改高危漏洞 402 个，中危漏洞 753 个，其余正在逐步开展整改工作。

信息化工作办公室一直对受攻击较严重的服务器进行重点关注，并通知到所受单位服务器系统管理员。对于危险性较高的漏洞，特别是应用系统漏洞，及时发现及时通知系统管理员整改。

校园网络安全隐患比较严重，全校应在管理和思想意识方面对网络安全引起足够重视。