中国地质大学（武汉）校园网络安全年报

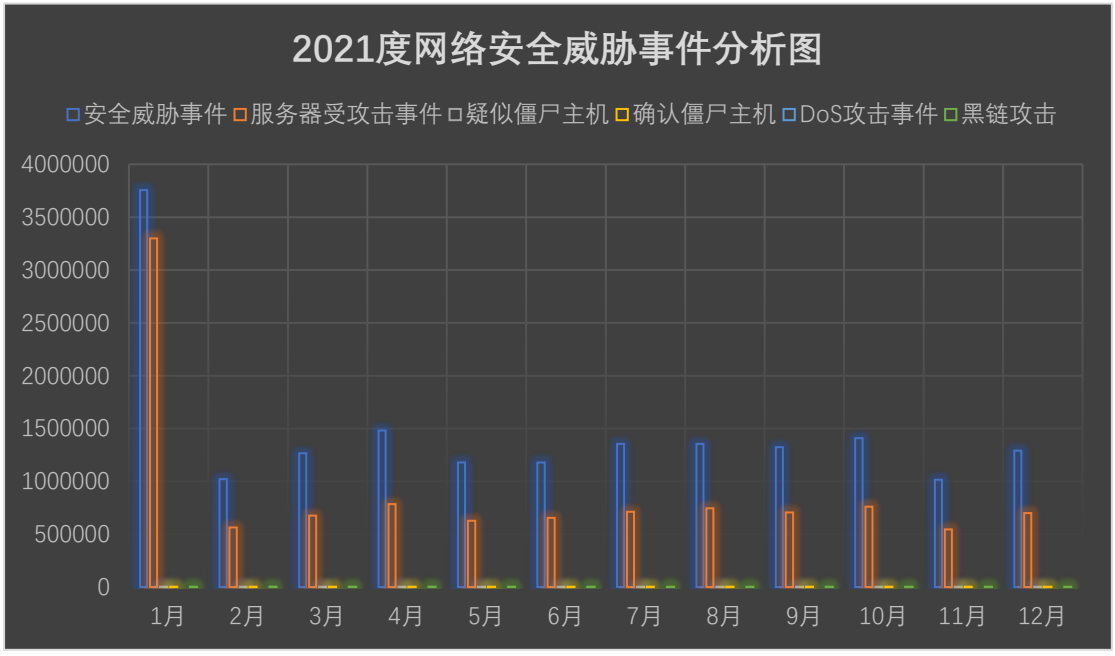
2021 年 12 月　　总第 4 期

中国地质大学（武汉）信息化工作办公室　　2022 年 1 月 10 日

1、情况综述

2021 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，2021 年校园网络发生的安全威胁事件 17626972 起、服务器受攻击威胁事件 10770073 起、疑似僵尸主机威胁事件 120 起、确认并处理僵尸主机威胁事件 119 起、DOS 攻击威胁事件 0 起、黑链威胁攻击事件 16 起。



2021年度安全监测数据统计表

月份	安全威胁事件	服务器受攻击事件	疑似僵尸主机	确认僵尸主机	DoS攻击事件	黑链攻击
1月	3756205	3297344	10	10	0	2
2月	1019579	562145	10	10	0	2
3月	1267558	675243	10	9	0	1
4月	1482236	785234	10	10	0	1
5月	1176974	626633	10	10	0	1
6月	1176974	653441	10	10	0	1
7月	1353751	712324	10	10	0	1
8月	1353751	745037	10	10	0	1
9月	1323748	706090	10	10	0	1
10月	1410036	761674	10	10	0	1
11月	1016226	546132	10	10	0	3
12月	1289934	698776	10	10	0	1

2、安全事件通报

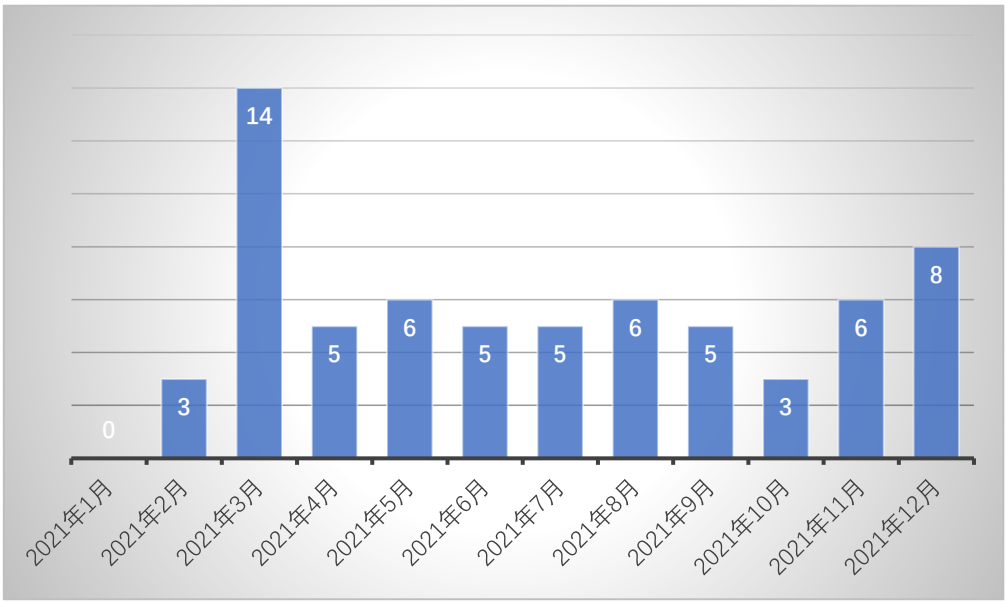
2021 年度信息化工作办公室共计发布预警 12 次，处理网络安全通报事件共 66 起；分别为：教育行业漏洞通报平台通报事件 34 起、湖北省网络与信息安全信息通报中心通报事件 12 起、教育系统网络安全工作管理平台通报事件 10 起、湖北省等保通报办公室通报事件 2 起、湖北省公安厅漏洞通报平台通报事件 1 起、湖北省网信办通报事件 1 起、关山街道办事处通报事件 1 起、喻家山派出所通报事件 1 起、其他通报事件 4 起。

具体内容如下：

2021 年度网络安全预警明细表

时间	内容
2021 年 1 月	关于爆发 incaseformat 病毒的预警通报
	关于 Sudo 堆缓冲区溢出漏洞的通报预警
2021 年 3 月	关于锐捷网络 EWEB 网管系统（EG 和 NBR 设备）存在远程命令执行漏洞的通报预警
	关于 Exchange 存在多个高危漏洞的通报预警
2021 年 4 月	关于 GitLab 存在任意文件读取漏洞的预警通报
	关于 Chrome 存在远程代码执行漏洞（0Day）的预警通报
2021 年 5 月	关于 VMware 发布安全补丁的的预警通报
2021 年 6 月	【安全通告】PHPMailer 远程代码执行漏洞
	关于 Windows Print Spooler 远程代码执行漏洞的预警通报
2021 年 7 月	关于 Weblogic 多个高危漏洞风险的预警通报
	关于 32 位 Redis 远程代码执行漏洞的预警通报
2021 年 8 月	关于 Microsoft 发布 2021 年 8 月安全更新的预警通报

2021 年度网络安全事件通报分析图



2021 年度网络安全事件汇总表

时间	日期	通报单位	内容	处理结果
2021 年 2 月	2 月 1 日	教育行业漏洞通报平台	学校某平台存在垂直越权漏洞	已整改
	2 月 20 日	教育系统网络安全工作管理平台	学校某信息系统存在未授权访问漏洞	已整改
	2 月 20 日	教育行业漏洞通报平台	学校某平台存在强制修改密码漏洞	已整改
2021 年 3 月	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某平台存在文件上传漏洞	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统存在弱密码问题	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统存在弱密码问题	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统信息泄露与弱密码问题	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统信息泄露与弱密码问题、SQL 注入	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统信息泄露与弱密码问题	已整改

	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统信息泄露与弱密码问题	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统弱密码信息泄露	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统弱密码信息泄露	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统弱密码信息泄露	已整改
	3 月 2 日	湖北省网络与信息安全信息通报中心	学校某信息系统弱密码信息泄露	已整改
	3 月 7 日	湖北省网络与信息安全信息通报中心	学校某信息存在任意文件读取漏洞	已整改
	3 月 11 日	教育系统网络安全工作管理平台	学校某信息系统双非弱密码	已整改
	3 月 21 日	教育行业漏洞通报平台、教育系统网络安全工作管理平台	学校某信息系统存在弱密码问题	已整改
2021 年 4 月	4 月 10 日	教育行业漏洞通报平台	学校某平台存在弱口令漏洞	已整改
	4 月 10 日	教育系统网络安全工作管理平台	学校某单位安全设备存在任意用户登录漏洞	已整改
	4 月 17 日	教育系统网络安全工作管理平台	学校某单位安全设备存在 Getshell 漏洞 14	已整改
	4 月 17 日	教育系统网络安全工作管理平台	学校某单位安全设备存在 Getshell 漏洞 125	已整改
	4 月 20 日	教育行业漏洞通报平台	学校某信息系统存在信息泄露漏洞问题	已整改
2021 年 5 月	5 月 6 日	教育行业漏洞通报平台	学校某用户存在遍历,未授权访问漏洞	已整改
	5 月 12 日	教育行业漏洞通报平台	学校某信息系统存在弱口令漏洞	已整改
	5 月 12 日	教育行业漏洞通报平台	学校某平台存在弱密码、任意文件上传漏洞	已整改

	5 月 23 日	教育行业漏洞通报平台	学校某平台存在网页 session 泄露问题	已整改
	5 月 24 日	教育行业漏洞通报平台	学校某平台存在弱口令、敏感信息泄露问题	已整改
	5 月 25 日	湖北省网信办	学校某信息系统存在敏感信息泄露问题	已整改
2021 年 6 月	6 月 2 日	教育行业漏洞通报平台	学校某信息系统存在信息泄露漏洞问题漏洞	已整改
	6 月 8 日	教育行业漏洞通报平台	学校某信息系统存在暗链漏洞问题	已整改
	6 月 8 日	教育行业漏洞通报平台	学校某信息系统存在暗链漏洞问题	已整改
	6 月 10 日	教育行业漏洞通报平台	学校某信息系统存在敏感信息泄露问题	已整改
	6 月 16 日	教育行业漏洞通报平台	学校某信息系统存在敏感信息泄露问题	已整改
2021 年 7 月	7 月 6 日	教育行业漏洞通报平台	学校某信息系统存在信息泄露漏洞问题	已整改
	7 月 8 日	教育行业漏洞通报平台	学校某信息系统存在弱口令漏洞问题	已整改
	7 月 8 日	教育行业漏洞通报平台	学校某信息系统存在任意文件读取漏洞问题	已整改
	7 月 12 日	教育行业漏洞通报平台	学校某信息系统存在任意文件上传漏洞问题	已整改
	7 月 20 日	教育行业漏洞通报平台	学校某信息系统存在信息泄露漏洞问题漏洞	已整改
2021 年 8 月	8 月 16 日	教育行业漏洞通报平台	学校某信息系统存在暗链问题	已整改
	8 月 17 日	教育行业漏洞通报平台	学校某信息系统存在身份证信息漏洞问题	已整改
	8 月 24 日	教育行业漏洞通报平台	学校某信息系统存在身份证信息泄露问题	已整改
	8 月 25 日	教育行业漏洞通报平台	学校某信息系统存在身份证信息泄露问题	已整改
	8 月 25 日	教育行业漏洞通报平台	学校某信息系统存在双非网站问题	已整改
	8 月 27 日	教育行业漏洞通报平台	学校某信息系统存在弱口令问题	已整改

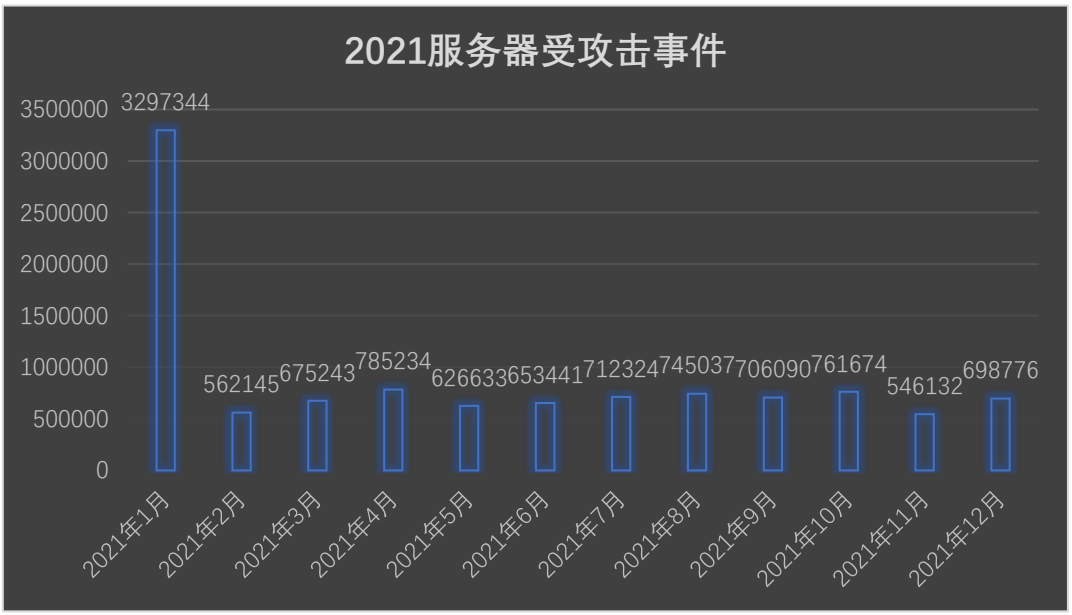
2021 年 9 月	9 月 2 日	教育行业漏洞通报平台	学校某信息系统存在代码执行问题	已整改
	9 月 3 日	教育行业漏洞通报平台	学校某信息系统存在代码执行问题	已整改
	9 月 13 日	教育行业漏洞通报平台	学校某信息系统存在敏感信息泄露问题	已整改
	9 月 18 日	教育行业漏洞通报平台	学校某信息系统存在敏感信息泄露问题	已整改
	9 月 24 日	教育行业漏洞通报平台	学校某信息系统存在双非网站，弱密码问题	已整改
2021 年 10 月	10 月 22 日	教育行业漏洞通报平台	学校某信息系统存在弱口令、敏感信息泄露问题	已整改
	10 月 22 日	教育行业漏洞通报平台	学校某信息系统存在弱口令问题	已整改
	10 月 22 日	教育行业漏洞通报平台	学校某信息系统存在弱口令问题	已整改
2021 年 11 月	11 月 4 号	湖北省公安厅漏洞通报平台	学校某信息系统存在弱口令问题	已整改
	11 月 15 号	教育系统网络安全工作管理平台	学校某信息系统存在敏感信息泄露问题	已整改
	11 月 15 号	教育系统网络安全工作管理平台	学校某信息系统存在外链问题	已整改
	11 月 26 号	教育系统网络安全工作管理平台	学校某信息系统存在暗链问题	已整改
	11 月 26 号	教育系统网络安全工作管理平台	学校某信息系统存在暗链问题	已整改
	11 月 29 号	第三方服务团队	某信息系统存在外链问题	督促整改
2021 年 12 月	12 月 9 号	湖北省等保通报办公室	学校某信息系统存在弱口令问题	已整改
	12 月 16 号	赛尔网络	学校疑似存在挖矿行为	已整改
	12 月 20 号	关山街道办事处通报	学校疑似存在挖矿行为	已整改
	12 月 22 日	喻家山派出所	学校某信息系统存在信息泄露问题	已整改
	12 月 23 号	赛尔网络	某信息系统存在外链问题	已整改
	12 月 23 号	赛尔网络	某信息系统存在外链问题	已整改
	12 月 30 号	教育系统网络安全工作管理平台	某信息系统存在暗链问题	已整改

	12 月 30 号	湖北省等保通报办公室	学校双非系统存在命令执行问题	已整改

3、服务器受攻击情况

2021 年度学校服务器受攻击事件共 10770073 起，平均月攻击次数为 897506 次，主要攻击类型网站扫描、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。

2021 年度学校服务器受攻击明细图



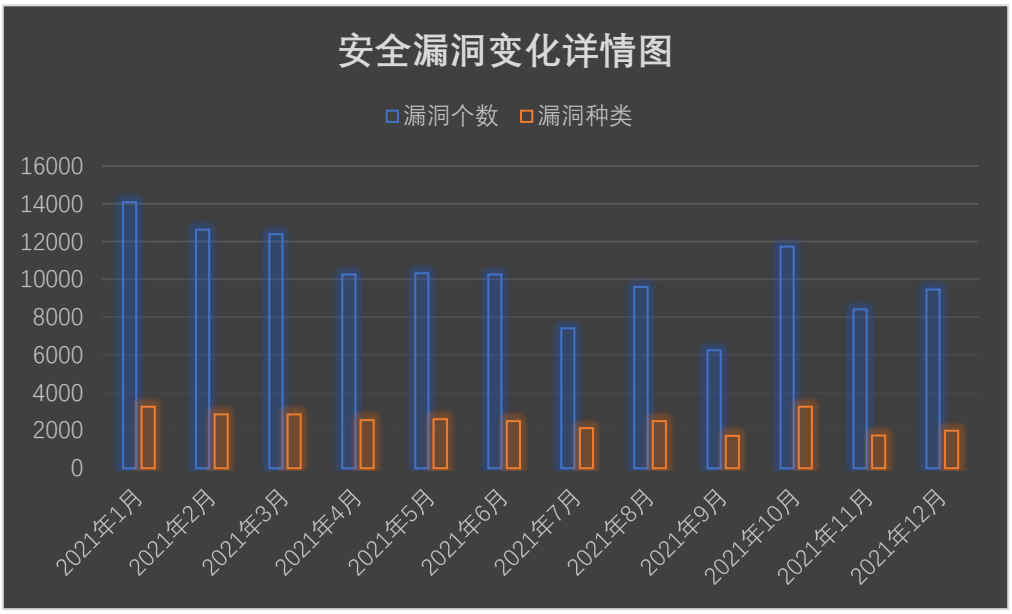
2021 年度学校服务器受攻击次数 TOP10 服务器列表

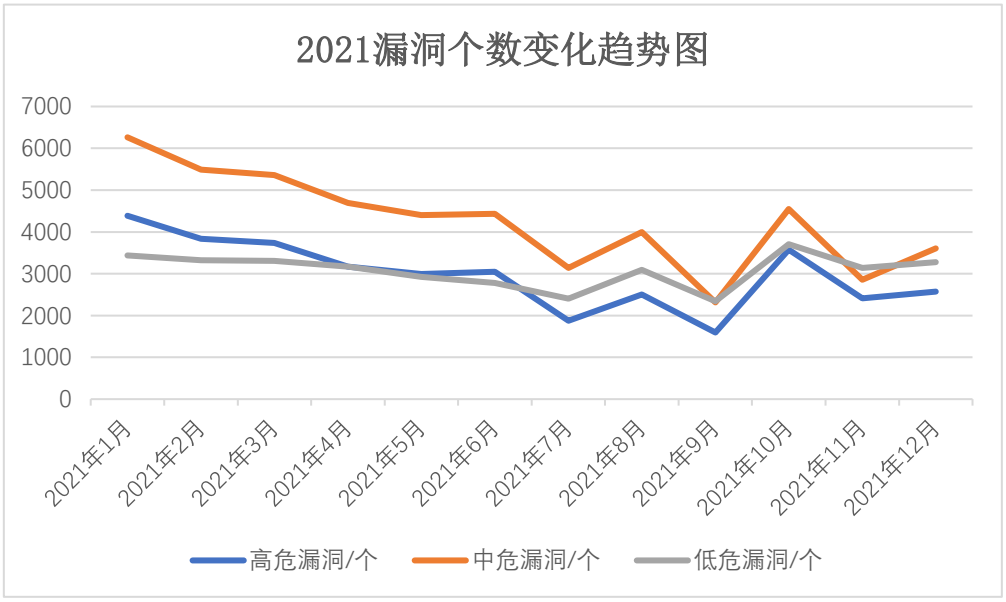
序号	目标服务器 IP/名称	所属单位	攻击次数
1	中国地质大学珠宝学院	珠宝学院	55976
2	湖北省学苑珠宝职业培训学校	珠宝学院	66063
3	地质科技情报	期刊社	330829
4	地球科学在线	期刊社	594695
5	中国地质大学出版社有限责任公司	中国地质大学出版社有限责任公司	117718
6	图书馆主页	图书馆	100577
7	校外访问平台	图书馆	21415
8	机构知识库	图书馆	12103

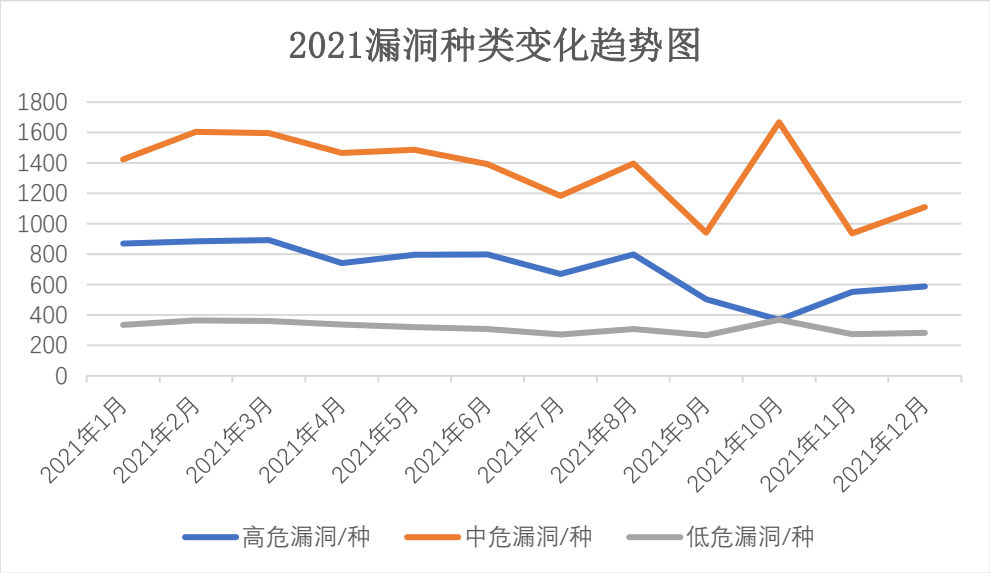
9	数字校园门户	信息化工作办公室	39011
10	采购管理信息系统	采购与招标管理中心	15567

4、服务器漏洞扫描分析

2021 年针对校园网服务器漏洞扫描检测工作成果如下：



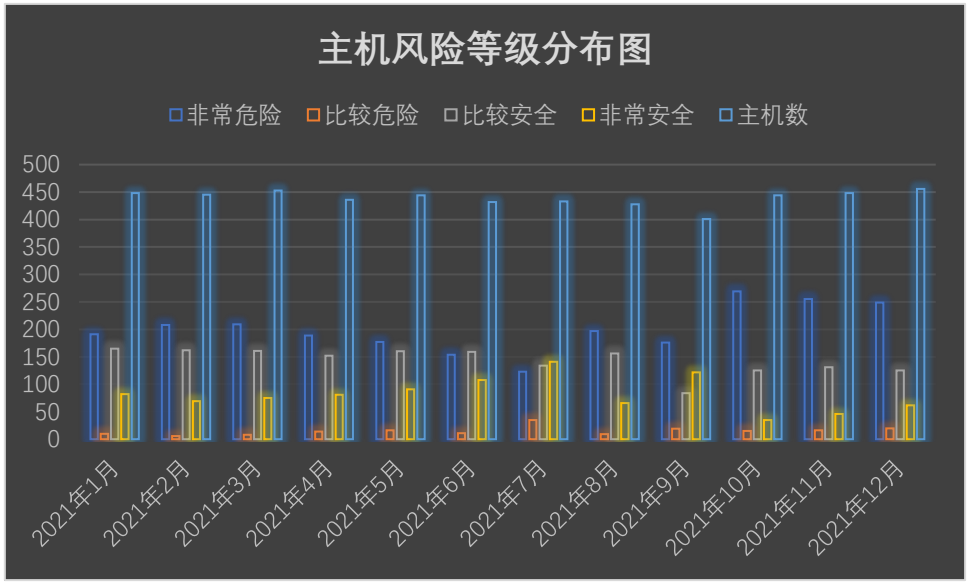




2021 年度主机风险等级分布表

时间	非常危险	比较危险	比较安全	非常安全	主机数
2021 年 1 月	191	10	165	82	448
2021 年 2 月	208	6	162	69	445
2021 年 3 月	209	8	161	75	453
2021 年 4 月	189	14	152	81	436
2021 年 5 月	177	16	160	91	444
2021 年 6 月	154	11	159	108	432
2021 年 7 月	123	35	134	141	433
2021 年 8 月	197	9	156	66	428
2021 年 9 月	176	19	84	122	401
2021 年 10 月	269	15	125	35	444
2021 年 11 月	255	16	131	46	448
2021 年 12 月	249	20	125	62	456

2021 年度主机风险等级分布图



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。2021 年度完成信息系统和网站漏洞扫描任务 470 次，复检 369 次，共下发系统整改通知书 698 份，邮件提醒督促漏洞整改工作 698 封。目前 80 余个系统完成漏洞整改，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。