中国地质大学（武汉）校园网络安全年报

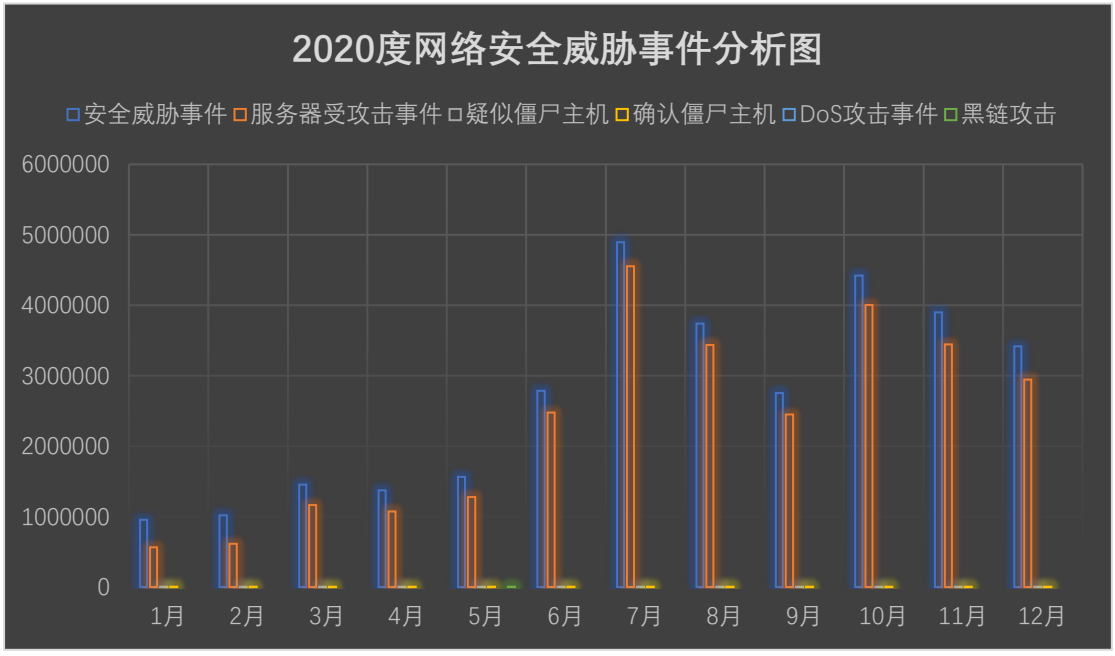
2020 年 12 月　　总第 3 期

中国地质大学（武汉）网络与信息中心　　2021 年 1 月 10 日

1、情况综述

2020 年我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，2020 年我校校园网络发生的安全威胁事件 32270922 起、服务器受攻击威胁事件 27995930 起、疑似僵尸主机威胁事件 154 起、确认并处理僵尸主机威胁事件 92 起、DOS 攻击威胁事件 0 起、黑链威胁攻击事件 4 起。



2020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	954503	564718	16	4	0	0
2月	1019986	611747	16	4	0	0
3月	1452923	1161462	16	4	0	0
4月	1373981	1071229	18	4	0	0
5月	1561896	1275482	10	2	0	2
6月	2784341	2478517	15	10	0	1
7月	4894824	4554316	17	12	0	0
8月	3739724	3433318	18	4	0	0
9月	2751536	2450305	4	13	0	0
10月	4421493	4002752	9	13	0	0
11月	3898236	3446112	5	12	0	0
12月	3417479	2945972	10	10	0	1

2、安全事件通报

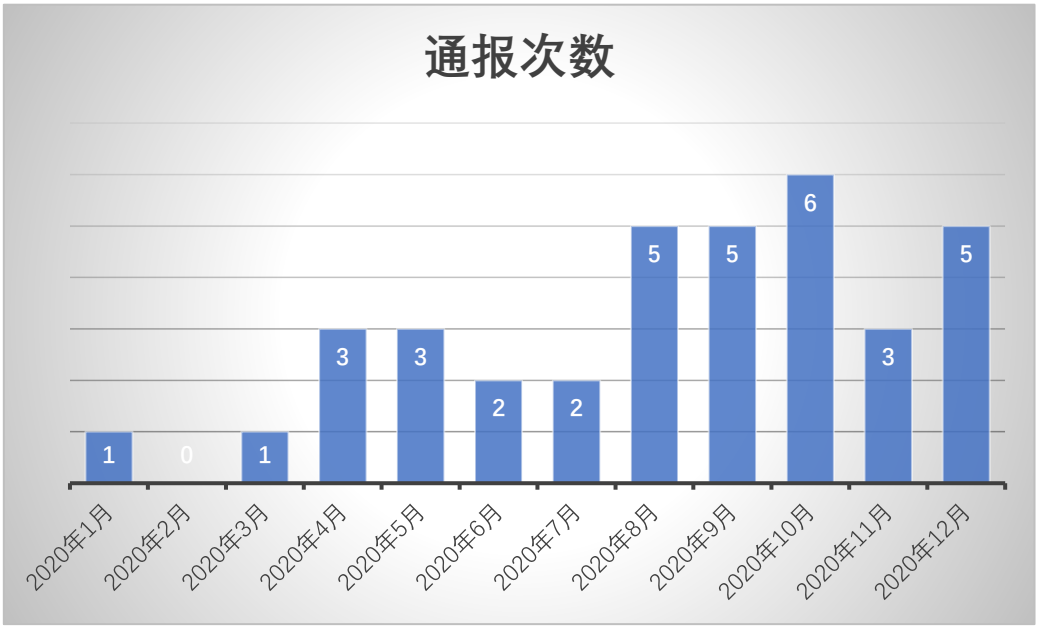
2020年度网络与信息中心共计发布预警16,处理网络安全通报事件共36起；分别为：教育行业漏洞平台通报 13 起、教育系统网络安全工作管理平通报事件 7 起、其他事件 16 起。

具体内容如下：

2020 年度网络安全预警明细表

时间	内容
2020 年 1 月	Windows SMBv3 客户端/服务器远程执行代码漏洞预警通知
2020 年 2 月	关于电脑版“新型冠状病毒”的通报预警
	关于匿名者黑客扬言攻击我国视频监控系统的通报预警
2020 年 3 月	Windows SMBv3 客户端/服务器远程执行代码漏洞预警通知
	通达 OA 高危漏洞可能感染勒索病毒的风险提示
2020 年 5 月	关于防范借‘两会’话题实施网络攻击的预警通报
	关于 SaltStack 软件存在高危漏洞的预警通报
2020 年 6 月	关于启明星辰运维安全网关存在高危漏洞的预警通报
2020 年 12 月	关于防范 Apache Struts 远程代码执行漏洞的预警通报
	关于 Microsoft 发布 2020 年 12 月安全更新的预警通报
	关于防范 Apache Shiro 权限绕过漏洞的预警通报
	关于防范 Tomcat WebSocket 拒绝服务漏洞的预警通报
	关于 Microsoft 发布 2020 年 11 月安全更新的预警通报
	关于防范 Cisco 多个产品存在高危漏洞的预警通报
	关于防范 Drupal 远程代码执行漏洞的预警通报
	关于防范 VMWare UAF 虚拟机逃逸漏洞的预警通报

2020 年度网络安全事件通报分析图



2020 年度网络安全事件汇总表

时间	通报单位	内容	处理结果
2020 年 1 月	教育行业漏洞报告平台	某系统存在弱口令	已整改
2020 年 3 月	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在弱口令漏洞	已整改
2020 年 4 月	教育部	某网站发表了不宜公开的文件	已删除
	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在外链指向赌博网站	已整改
	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在外链指向赌博网站	已整改
2020 年 5 月	教育系统网络安全工作管理平台安全监测预警子系统	某网站存在未授权访问	已整改
	教育部	某系统 redis 未授权访问漏洞	已整改
	校内安全维稳	协助处置校园舆情事件	已处理
2020 年 6 月	教育系统网络安全工作管理平台	某网站存在敏感信息泄露	已删除
	教育部	某 APP 存在后门-app 安全威胁	已整改
2020 年 7 月	教育行业漏洞平台	某网站存在文件上传漏洞	已整改
	教育行业漏洞平台	某系统存在弱密码漏洞	已整改

2020 年 8 月	教育行业漏洞报告平台	某系统存在越权查看他人信息漏洞	已整改
	教育行业漏洞报告平台	某学院存在敏感信息泄露问题	已整改
	教育行业漏洞报告平台	某单位存在弱密码和逻辑漏洞	已整改
	湖北省教育厅网信办	某网站出现涉黄信息	已协助处理
	教育行业漏洞平台	某教师收到钓鱼邮件	已删除
2020 年 9 月	教育行业漏洞报告平台	某系统存在 SSRF 漏洞问题	已整改
	校内安全维稳	协助处置校内舆情事件	已处理
	教育行业漏洞报告平台	某系统存在弱口令问题	已整改
	教育行业漏洞报告平台	某系统存在弱口令问题	已整改
	教育系统网络安全工作管理平台安全监测预警子系统	某系统存在弱口令问题	已整改
2020 年 10 月	教育行业漏洞报告平台	某系统存在文件上传导致 XSS 漏洞问题	已整改
	教育行业漏洞报告平台	某学院绩效管理系统 SQL 注入问题	已整改
	教育行业漏洞报告平台	某系统存在敏感信息泄露问题	已整改
	教育网	某机房电脑存在访问恶意 IP 问题	已整改
	校内安全维稳	学生在微博发布不良言论	已协助处理
	校内安全维稳	协助处置校内舆情事件	已协助处理
2020 年 11 月	中国教育和科研计算机网	某学院机房电脑存在访问恶意 IP 问题	已整改
	教育系统网络安全工作管理平台	某系统存在任意文件下载漏洞	已整改
	省委网信办	某单位宣传材料内容有误	已整改
2020 年 12 月	湖北省网络与信息安全信息通报中心	某系统存在任意文件下载漏洞	已整改
	校内安全维稳	协助处置校内舆情问题	已处理

	教育网	12 月 25 日，某机房电脑访问恶意 IP 问题	已整改
	省教育厅	协助处置舆情问题	已处理
	教育网	12 月 30 日，某机房电脑访问恶意 IP 问题	已整改

3、服务器受攻击情况

2020 年度学校服务器受攻击事件共 27995930 起，平均月攻击次数为 2332994 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。

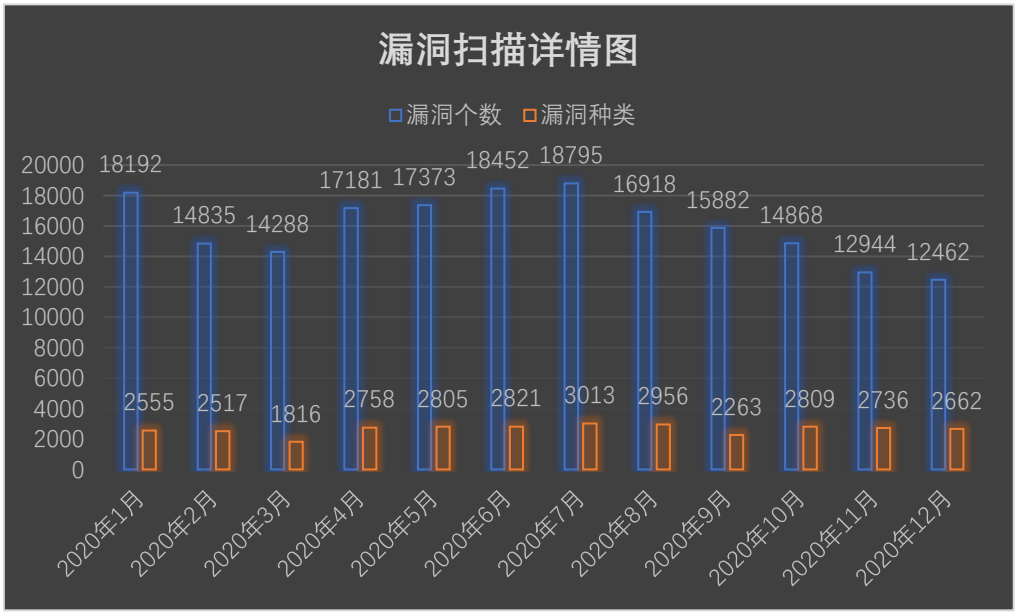
2020 年度学校服务器受攻击明细图

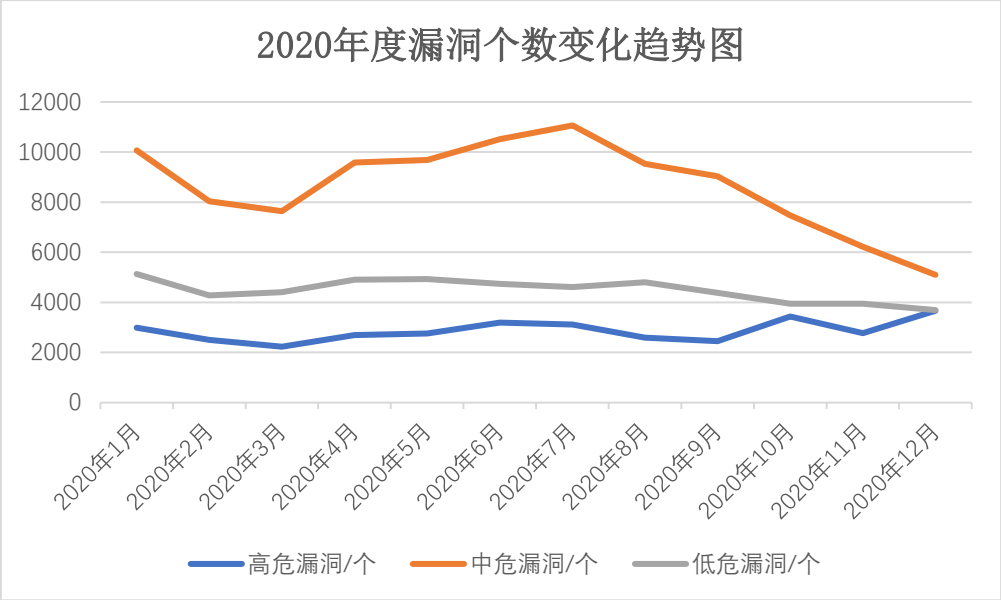
2020 年度学校服务器受攻击次数 TOP10 服务器列表

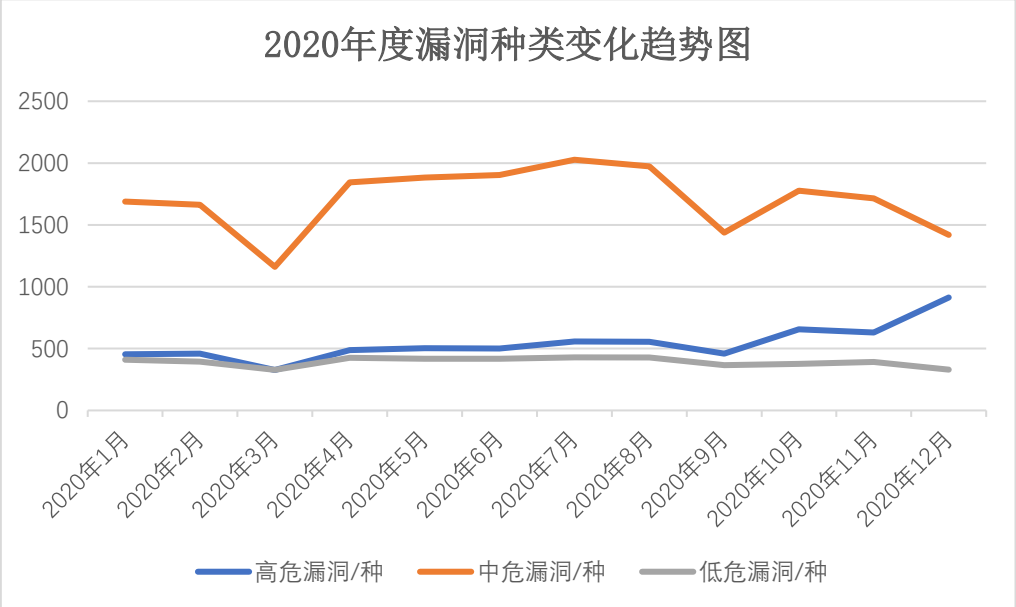
序号	目标服务器 IP/名称	所属单位	攻击次数
1	站群系统	网络与信息中心	3004369
2	第一站群系统	网络与信息中心	2843914
3	教师个人主页发布系统	教师个人主页发布系统	504964
4	第二站群系统	网络与信息中心	309097
5	校园虚拟专用网络（VPN）	网络与信息中心	270418
6	地球科学在线	期刊社	248958
7	图书馆主页	图书馆	122064
8	地质科技情报	期刊社	126282
9	中国地质大学出版社有限责任公司（含中国地质大学出版社职教分社）	中国地质大学出版社有限责任公司	83661
10	检测数据查询	中国地质大学珠宝学院	80046

4、服务器漏洞扫描分析

2020 年针对校园网服务器漏洞扫描检测工作成果如下：



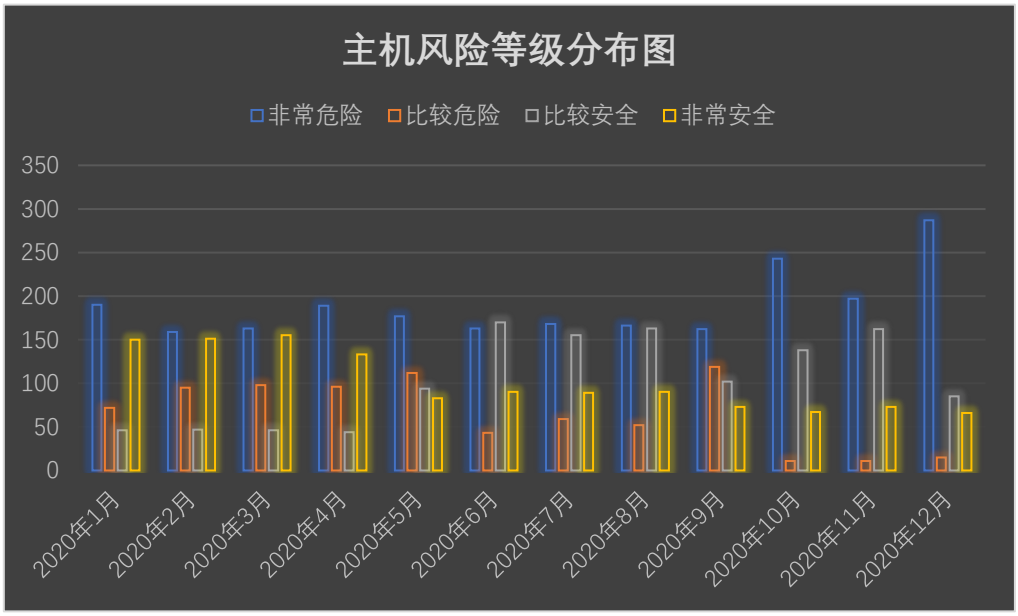

2020年度漏洞个数变化趋势图
12000
10000
8000
6000
4000
2000
0
2020年1月
2020年2月
2020年3月
2020年4月
2020年5月
2020年6月
2020年7月
2020年8月
2020年9月
2020年10月
2020年11月
2020年12月
高危漏洞/个
中危漏洞/个
低危漏洞/个


2020年度漏洞种类变化趋势图
2500
2000
1500
1000
500
0
2020年1月
2020年2月
2020年3月
2020年4月
2020年5月
2020年6月
2020年7月
2020年8月
2020年9月
2020年10月
2020年11月
2020年12月
高危漏洞/种
中危漏洞/种
低危漏洞/种

2020 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
2020 年 1 月	190	72	46	150	458
2020 年 2 月	159	95	47	151	452
2020 年 3 月	163	98	46	155	462
2020 年 4 月	189	96	44	133	462
2020 年 5 月	177	112	94	83	466
2020 年 6 月	163	43	170	90	466
2020 年 7 月	168	59	155	89	471
2020 年 8 月	166	52	163	90	471
2020 年 9 月	162	119	102	73	456
2020 年 10 月	243	11	138	67	459
2020 年 11 月	197	11	162	73	443
2020 年 12 月	287	15	85	66	453

2020 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。网络与信息中心根据“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网络与信息中心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

网络与信息中心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。2020 年度完成信息系统和网站漏洞扫描任务 975 次，复检 285 次，共下发系统整改通知书 805 份，邮件提醒督促漏洞整改工作 805 封。目前 69 个系统完成漏洞整改，其余正在逐步开展整改工作。

网络与信息中心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。