中国地质大学（武汉）网络安全月报

2020 年 04 月　（第 W0050 期）　总第 50 期

中国地质大学（武汉）网络与信息中心　2020 年 04 月 30 日

1、情况综述

根据监测分析，4 月份我校校园网络发生的安全威胁事件共计 1373981 起，其中服务器受到攻击的事件共计 1071229 起；网站受到攻击的事件共计 302752 起；可能感染病毒木马的僵尸主机共 18 台，其中确定的僵尸主机共 4 台；对外发生的 DoS 攻击事件 0 起，被植入黑链的网站共 0 个。

4 月份我校总体网络安全情况良好，处理网络安全事件共 2 起，未发生重大的网络安全事件,后续会继续保持和完善。

2、安全事件通报

4 月处理网络安全事件共 2 起。教育系统网络安全工作管理平台通报事件 2 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	4 月 9 日	接上级部门通报某学院网站存在非法外链。	已整改
2	4 月 10 日	接上级部门通报某学院网站存在非法外链。	已整改

3、服务器受攻击情况

本次监测时间为 4 月，防火墙防护服务器受到攻击事件共1071229 起;其中针对学校门户站群系统的攻击次数达到 415252 起，占总数的 38.8%。门户站群系统提供我校 140 个各类网站的管理、发布功能，可以有效防护攻击，保障网站安全。

受攻击次数排名前十的服务器列表

序号	目标服务器名称	攻击次数	百分比
1	站群系统	415252	38.8%
2	地球科学在线	22152	2.1%
3	图书馆主页	11041	1%
4	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）	8931	0.8%
5	研究生管理信息系统	7641	0.7%
6	检测数据查询	7007	0.7%
7	校外访问平台	6047	0.6%
8	教师个人主页发布系统	4184	0.4%
9	中国地质大学校园虚拟专用网络（VPN）服务	3769	0.4%
10	远程教学管理平台	3743	0.3%
11	其他	581467	54.3%
12	所有	1071229	100%

4、服务器漏洞扫描分析

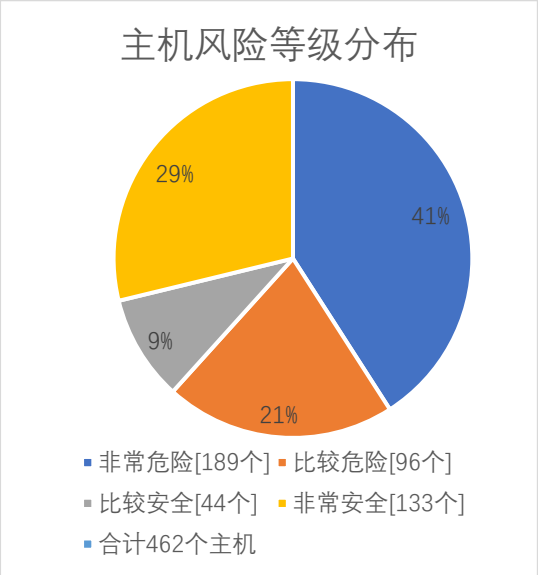
根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。网络与信息中心将督促各单位进行系统漏洞整改，对于严重高危漏洞将采取互联网防火墙策略收缩，限制部分存在严重高危漏洞的服务器访问权限，整改后上报网络与信息中心进行复检。

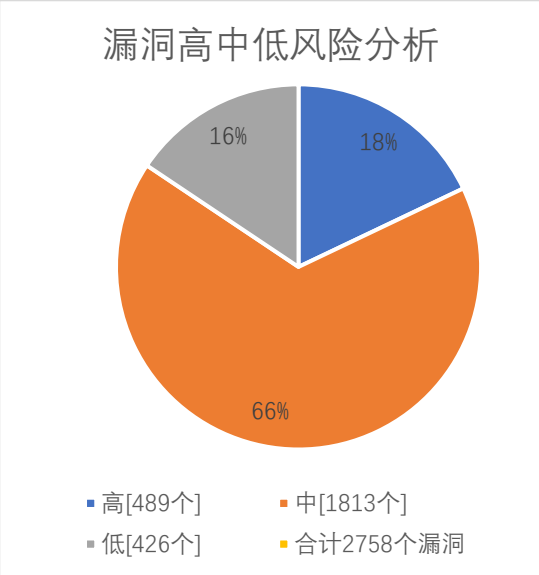
本月漏洞数量较上月明显增多，4 月将继续严抓漏洞整改工作，采取“管技结合”的方式，督促各单位尽快修复漏洞，并上报网络与信息中心进行复检，保证正常工作用网安全。

漏洞数量	主机高危	主机中危	主机低危	合计
3 月份	2233	7643	4412	14288
4 月份	2694	9579	4908	17181
变化量（个）	+461	+1936	+496	+2893

漏洞种类	主机高危	主机中危	主机低危	合计
3 月份	327	1161	328	1816
4 月份	489	1843	426	2758
变化量（种）	+162	+682	+98	+942

在本月扫描的 463 台服务器中，主机漏洞共计 2758 种，主机漏洞总计 17181 个。其中高危漏洞 489 种，总计 2694 个；中危漏洞 1843 种，总计 9579 个；低危漏洞 426 种，总计 4908 个。主机风险等级中，非常危险的占 41%，比较危险的占 21%，比较安全的占 9%，非常安全的占 29%。漏洞风险等级中，高危漏洞占比 18%，中危漏洞占比 66%，低危漏洞占比 16%。





5、安全漏洞整改情况

4 月网络与信息中心针对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。相比于 3 月，本月漏洞库更新，漏洞种类增多，其中系统漏洞类型增多 17740 种，web 漏洞类型增多 2 种。根据数据分析，由于有主机漏洞增多，导致高危漏洞数量增多。

对比 3 月，本月高危漏洞类型增加 162 种，高危漏洞个数增加 461 个，总的漏洞类型增加 942 种，总的漏洞数量增加 2893 个。

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。

校园网络内部安全隐患比较严重，全校应在网络安全管理和意识方面引起足够重视。