中国地质大学校园网络安全月报

2018 年 8 月　　（第 2018-08 期）　总第 32 期

中国地质大学（武汉）网络与信息中心　　2018 年 9 月 10 日

1、情况综述

2018 年 8 月 1 日至 2018 年 8 月 31 日，我校总体网络安全情况良好，未发生重大的网络安全事件。

8 月份，网络与信息中心对服务器所在的 8 个 C 类地址段进行了全方位的漏洞扫描。根据监测分析，我校校园网络发生的安全威胁事件共 516320 起，服务器受到攻击的事件共 288856 起;可能感染病毒木马的僵尸主机共 42 台，其中确定的僵尸主机共 29 台；对外发生的 DoS 攻击事件共 0 起，被植入黑链的网站共 0 个。

2、安全事件通报

8 月收到并处理网络安全事件通报 5 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2018-8-5	一门户网站存在上传文件权限漏洞	已修复
2	2018-8-6	一系统存在单点登录安全漏洞	已修复
3	2018-8-7	一门户网站存在单点登录安全漏洞	已修复
4	2018-8-11	一应用系统存在未授权用户登录安全漏洞	已修复
5	2018-8-17	一二级单位自建校外网站存在 SQL 注入安全漏洞	已关停外网网站

3、用户终端情况

本月对校园网有线接入用户终端（以办公电脑为主）进行主动安全扫描。扫描识别 596 台终端用户设备。发现漏洞 351 个，其中高危漏洞 129 个，严重漏洞 222 个。以 Windows 系统安全漏洞为主，建议用户及时更新 Windows 补丁。

危害排名前五的漏洞列表

序号	名称	危害程度	主机数量
1	Microsoft Windows XP Unsupported Istallation	高危	47
2	MS17-010:Microsoft Windows SMB	高危	34
3	Web Server Directiry Traversal Arbitrary File	高危	5
4	MS14-066:Vulnerability in Schannel Could Allow	高危	8
5	MS15-034:Vlulnerability in HTTP sys Could Allow	高危	4

4、服务器受攻击情况

本月服务器受到攻击事件共 288856 起，较 7 月份呈上升趋势。其中针对学校门户站群系统的攻击次数达到 177961 起，占总数的 61.6%。门户站群系统提供我校 111 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

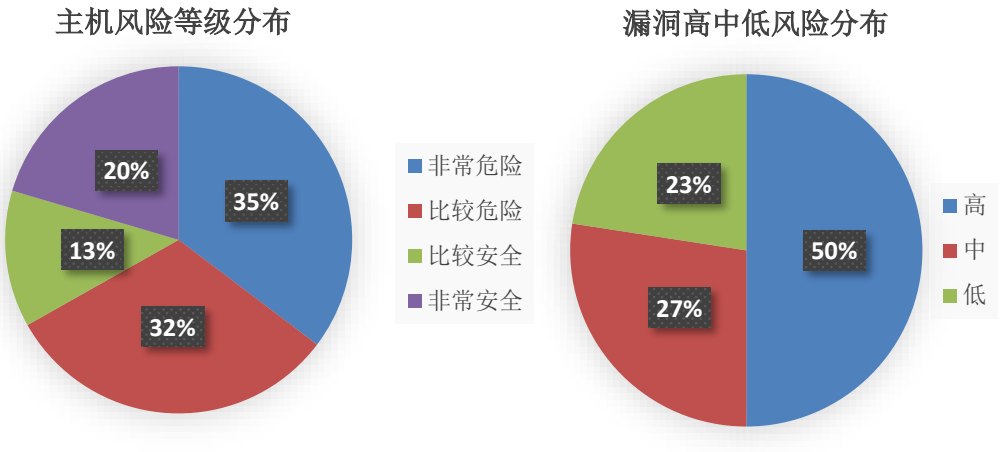
序号	网站	受到攻击次数	备注
1	学校门户站群系统	177961	
2	图书馆主页	11282	
3	远教学院主页	9698	
4	二级单位主页服务	9049	
5	网页反向代理服务器	7285	
6	计算机学院主页	4911	
7	地球科学期刊主页	4723	
8	图书馆查新检索服务器	3717	
9	环境学院所属网站	3604	
10	期刊社采编服务系统	3544	
11	其他	52542	
总计		**288856**	

5、服务器漏洞扫描分析

本月对校园网服务器所在的 8 个 C 类地址网段进行漏洞扫描结果统计如下：共发现高危漏洞 339 个，中危漏洞 186 个，低危漏洞 153 个。

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。

在扫描的近 500 台服务器中，主机风险等级中，非常危险的占 35%，比较危险的占 32%，比较安全的占 13%，非常安全的仅占 20%。高风险漏洞占 50%。



6、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，其中 48 个危险系数较高的重点业务系统，23 个系统整改完毕，23 个系统正在整改中，2 个系统因业务调整关闭。其它中低危险漏洞的服务器正在整改中。

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，学校应在管理和意识方面对网络安全引起足够重视。

中国地质大学校园网络运行月报

2018 年 7-8 月　　（第 2018-01 期）　总第 1 期

中国地质大学（武汉）网络与信息中心　　2018 年 9 月 10 日

1、校园网络运行情况

7 月份校园网活跃用户数为 25153 人，其中校园宽带用户 19845 人，联通宽带用户 3110 人，移动宽带用户 2198 人。新开户 149 人，其中校园宽带用户 89 人，联通宽带用户 12 人，移动宽带用户 48 人。校园宽带用户使用流量总计为 143.83TB。

8 月份校园网活跃用户数为 19043 人，其中校园宽带用户 15925 人，联通宽带用户 1950 人，移动宽带用户 1168 人。新开户 218 人，其中校园宽带用户 102 人，联通宽带用户 20 人，移动宽带用户 96 人。校园宽带用户使用流量总计为 100.04TB。

7-8 月无线网络用户最大连接数 9971 人，其中思科无线网络用户最大连接数 7059 人，Aruba 无线网络用户最大连接数 2912 人。7-8 月校园宽带教育网出口平均流量 753.99Mbps，峰值为 2020Mbps，高峰时段（10:00-24:00）网络带宽使用率超过 95%。电信网出口平均流量 273.43Mbps，峰值为 959.16Mbps。高峰时段（10:00-24:00）网络带宽使用率超过 50%。

中心利用暑期开展了设备巡检自查工作。巡检主干核心网络设备 25 台，数据中心网络设备 24 台，各设备运行正常，未发现风险隐患。巡检网络安全设备 8 台，排除许可授权过期隐患 2 处、日志数据过量风险 1 处。

2、网络安全

7 月份校园网络发生的安全威胁事件共 256963 起，服务器受到攻击的事件共 165215 起；可能感染病毒木马的僵尸主机共 42 台，其中确定的僵尸主机共 29 台；对外发生的 DoS 攻击事件共 0 起，被植入黑链的网站共 1 个。收到并处置“教育系统网络安全工作管理平台”通报网络安全事件共 1 起。

8 月份，校园网络发生的安全威胁事件共 516320 起，服务器受到攻击的事件共 288856 起；可能感染病毒木马的僵尸主机共 42 台，其中确定的僵尸主机共 29 台；对外发生的 DoS 攻击事件共 0 起，被植入黑链的网站共 0 个。收到并处置“教育行业漏洞报告平台”通报网络安全事件共 5 起。

为准确掌握校园网络安全情况，中心于 8 月份对校园网服务器所在的 8 个 C 类地址网段进行漏洞扫描，共发现高危漏洞 339 个，中危漏洞 186 个，低危漏洞 153 个。同时对涉及的 48 个危险系数较高的重点业务系统提出了具体的整改意见和建议，

23 个系统整改完毕，23 个系统正在整改中，2 个系统因业务调整关闭。其它中、低危险漏洞的服务器正在整改中。

我校虽未发生重大的网络安全事件，但内网网络安全隐患突出。

3、网络用户服务

7 月份故障报修共计 32 起：有线网络故障 17 起，其中装修引起的链路故障近一半，办公室没有布线的 2 起，网络设置问题 2 起；无线网络故障 15 起，其中 8 起是用户没有登陆 3A，4 起是欠费，3 起是合作方移动或联通的问题；网络咨询 18 起，修改邮箱密码 10 次。

7 月份新增邮箱用户 12 个。活跃邮箱（月登录 31 次以上）用户 3607 个，常用用户（月登录 11-30 次）1709 个。接收外域邮件总量 138493 封，发送外域邮件总量 14763 封，域内邮件接收总量 11699 封，总计 164955 封。

8 月份故障报修共计 36 起：有线网络故障 19 起，其中 12 起是由于交换机端口故障引起的，3 起是墙面面板故障，4 起是误报；无线网络故障 17 起，其中 5 起是用户没有登陆 3A，3 起是欠费，3 起是合作方移动或联通的问题， 6 起是雷击导致 AP 损坏，修改邮箱密码 5 次。新校区机房内光纤尾纤被老鼠咬断，紧急维修 2 次。新综合楼至研究生院光纤被校内施工挖断。

8 月份新增邮箱用户 1 个。活跃邮箱（月登录 31 次以上）用户 4713 个，常用用户（月登录 11-30 次）538 个。接收外域邮件总量 140982 封，发送外域邮件总量 11196 封，域内邮件接收总量 9334 封，总计 161512 封。

完成了水工楼前楼、结构楼、三峡中心、煤工系、教一楼、青藏中心、学工处、西区体育馆、主楼东、珠宝楼、教务处、材化学院等 12 栋楼的网络设备机房的设备维护和线路整理，更换机柜 4 个，更换标签 2000 余个，整理点位 937 个。完成了假期对 41 栋粉刷装修的学生宿舍内的无线 AP 的保护工作，涉及的无线 AP 设备 875 个；对办公区区域交换机实施保护 6 台，无线 AP 更换 34 台。完成了教务处楼房的光缆入地工作。

完成了中心机房到各楼栋的汇聚交换机的更换准备工作，对交换机对应楼栋的每个端口进行了配置检查和登记工作，共计交换机七台、端口 192 个。

圆满完成了学校 7 月份的秋季招生的网络保障工作，学校 9 月份迎新的网络保障准备工作已经就绪。

8 月份部分网络设备遭雷击，已确认受影响的无线 AP 设备有 144 颗并已全部更换。

4、高性能计算

高性能计算平台保持正常运行的计算节点有 43 个，现有用户数 68 个。7 月 26 日停电事件造成 1 个存储控制器和 6 个计算节点损坏。

完成用户作业情况：7-8 月累计完成用户作业总数为 14041 个，7 月份完成用户作业 12510 个，8 月份完成用户作业 1531 个。

计算核心使用情况：7-8 月累计使用计算核心总数为 116414 核，7 月份使用计算核心数为 109217 核，8 月份使用计算核心为 7197 核。

CPU 使用时间情况：7-8 月累计完成 CPU 机时 476886.06 小时，有效率为 73.16%。7 份 CPU 使用时间为 289115.7028 小时，8 月份 CPU 使用时间为 187750.3586 小时。

WallTime 时间情况：7-8 月累计 WallTime 为 651785.4943 小时。其中，7 月份 WallTime 时间为 341689.7904 小时，8 月份，WallTime 时间为 310095.7039 小时。

内存使用情况：7-8 月累计使用内存为 1.9355337TB。其中，7 月份内存使用为 1.8048383TB，8 月份内存使用为 0.1306993TB。

已使用共享存储总量 350.54TB，剩余 322.33TB。

5、一卡通运行

学校现有校园卡用户 59284 人，其中各类学生用户 42223 人，教职工用户 5079 人，临时卡用户 11981 人。

7 月份自助补卡 268 张；自助圈存 71192 次，人工充值 7210 次，其中网上和微信圈存 4011 次，手机 APP 圈存 4853 次，圈存机圈存 62328 次；消费总次数 77.5 万次。

对全校所有一卡通设备及线路进行日常巡检 2 次；自助补卡机加卡 6 次，更换打印色带 3 次；处理刷卡 POS 机故障 3 次；处理圈存机故障 3 次；处理自助补卡机故障 1 次；7 月 26 日的停电造成一卡通服务器全部意外断电并终止服务，经过近一周的设备维修、调试，恢复正常运行。

8 月份自助补卡 182 张；自助圈存 41355 次，人工充值 5947 次，其中微信圈存 1050 次，手机 APP 圈存 2460 次，自助线下圈存机圈存 37845 次；消费总计 53 万次。

对全校所有一卡通设备及线路进行日常巡检 2 次；自助补卡机加卡 4 次，更换打印色带 2 次；处理刷卡 POS 机故障 3 次；处理圈存机故障 4 次；处理自助补卡机故障 1 次；处置北区食堂二楼施工导致电路故障 1 次，处置因雷雨天气致学三食堂电路故障 1 次。

发现一卡通系统安全漏洞，已关闭外网访问功能，正在进行漏洞修补和相关安全测试。

6、校园信息化

截至 8 月底，校园信息门户系统已接入业务系统 35 个，其中已实现单点登录的业务系统 20 个。

校园网络已认证用户总数 35639 人，其中教职工 3325 人，本科生 18235 人，研究生 9969 人，非全日制研究生 561 人，留学生 805 人，后勤聘用人员 954 人，离退休人员 1711 人。

7 月份访问信息门户人数为 18529 人次，8 月份访问信息门户人数为 13833 人次，7-8 月访问共计 32362 人次。开通微信门户用户总数为 21168 人，总访问量为 36649 人次，日均访问量为 591 人次。

网上办事大厅创建服务 37 项，已办结事项 8 项。7 月份办事大厅访问量为 2971 人次，8 月份办事大厅访问量为 1172 人次，7-8 月办事大厅总访问量为 4143 人次。

数据中心提供数据共享服务 18 项。

站群管理系统运行的网站 111 个。暑假期间完成了两学一做专题网、区域经济与投资环境研究中心、结晶学与矿物学科普网站 3 个网站的迁移工作；完成了 MBA 教育中心网站的改版工作。站群系统遭受 1151 次入侵攻击，封禁非法操作账户 4 次。

7、突发事件

2018 年 7 月 26 日凌晨网络中心机房供电双回路 ATS 均被切断（实际停电时间 02:24 至 04:51），UPS 电量耗尽后整个机房于 04:23 断电，从而导致中心机房内所有设备异常断电停机，导致大批网络设备和服务器终止服务，并造成数据丢失和设备故障，经过近一周的设备维修和故障恢复处理，学校公共服务基础设施所承担的服务绝大部分恢复正常。28 日再次停电时，采用租借的 500KW 柴油发电机组，保障了网络的供电，避免了设备因停电冲击造成的损坏。

据初步统计，造成的直接损失包括：远程与继续教育学院 3 个存储控制器更换需 8 万元，数据恢复需 3 万元；高性能计算存储控制卡更换需 1.8 万元；相关网络设备需更换，共约 2 万元；MD3000 磁盘故障 2 块，控制卡故障 1 块，损失达 1.6 万元；Oracle ODA 数据库一体机计算节点的两条内存烧坏以及 NETAPP 存储的 16G FC 网卡烧坏，损失估计 3.8 万元；6 个计算节点 node53、node59、node60、node66、node79、node56 重新开机后设备无法正常启动的损失不计算在内，按购买设备原价价格计算约 30 万元。精密空调在保修范围内未计损失。损失共计约达 50.2 万元。