中国地质大学网络安全月报

2019 年 01 月-02 月　（第 W0038 期）（发布）　总第 38 期

中国地质大学（武汉）网络与信息中心　2019 年 3 月 6 日

1、情况综述

根据监测分析，1-2 月份我校校园网络发生的安全威胁事件共计 1309454 起，其中 1 月 690827 起、2 月 618627 起，服务器受到攻击的事件共计 452281 起，其中 1 月 218453 起、2 月 233828 起;可能感染病毒木马的僵尸主机共 31 台，其中确定的僵尸主机共 24 台；对外发生的 DoS 攻击事件共 0 起，被植入黑链的网站共 2 个。

本月我校总体网络安全情况良好，处理网络安全事件共 3 起，未发生重大的网络安全事件。

2、安全事件通报

1-2 月处理网络安全事件共 3 起。其中，教育部通报 2 起、校内安全维稳 1 起。

网络安全事件汇总表

序号	时间	内容	处理结果
1	2019-1-11	一网站源代码泄露安全漏洞	已修复
2	2019-2-25	一网站黑链漏洞	已修复
3	2019-2-28	协助处理校内舆情事件	已完成

3、用户终端情况

本次用户终端安全监测针对 1 月-2 月，对校园网有线接入用户终端（59.71.224.0-59.71.255.255）进行主动安全扫描。扫描识别到 674 台终端用户设备。发现漏洞 355 个，其中高危漏洞 132 个，严

重漏洞 223 个。以 Windows 系统安全漏洞为主，建议用户及时更新 Windows 操作系统以及相关系统补丁。

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 不支持的安装检测	严重	39
2	Microsoft Windows SMBv1 多个漏洞	严重	39
3	MS17-010:Microsoft Windows SMB	严重	36
4	CriticalIntel 管理引擎不安全读写操作 RCE (INTEL-SA-00075)	严重	9
5	MS12-020:远程桌面中的漏洞可允许远程代码执行	高危	13

4、服务器受攻击情况

本次监测时间为 1 月-2 月，服务器受到攻击事件共 452281 起；其中针对学校门户站群系统的攻击次数达到 250522 起，占总数的 55.3%。门户站群系统提供我校 117 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	主机名称	受到攻击次数
1	学校门户站群系统	250522
2	地质科技情报编辑部网站	31045
3	地球科学期刊服务器	14671
4	远教学院微信平台	14988
5	计算机学院主页	6230
6	网络中心反向代理服务器	12524
7	图书馆服务器主页	8505
8	校办二级单位主页服务器	8613
9	教职工个人主页	3371
10	远教学院教学平台	7168
11	其他	36617
总计		**394254**

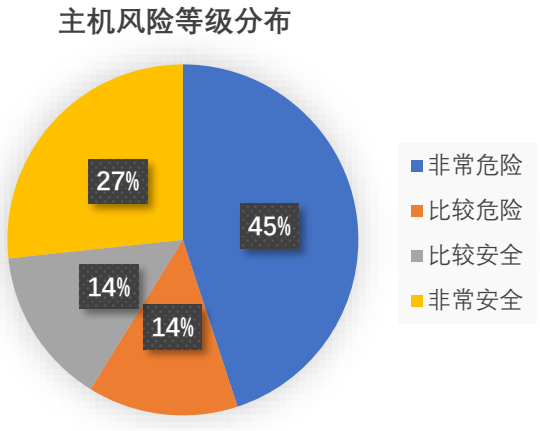
5、服务器漏洞扫描分析

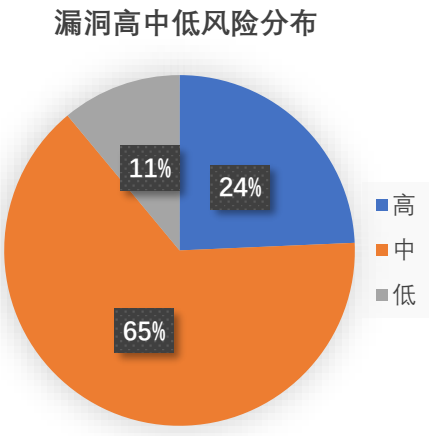
寒假期间中心组织开展对学校数据中心的全面安全漏洞扫描检测。结果统计如下：共发现高危漏洞 897 个，中危漏洞 2386 个，低危漏洞 688 个。

根据监测分析，黑客攻击校园网络的主要方式为漏洞攻击。1 月-2 月采取寒假期间安排安全值班，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，督促各单位做好寒假期间网络安全预防措施，保证寒假期间各单位用网安全。

3 月将加大漏洞整改工作力度，督促各单位尽快修复漏洞，并上报网络中心进行复检，保证正常工作用网安全。

在扫描的 475 台服务器中，主机风险等级中，非常危险的占 45.1%，比较危险的占 13.8%，比较安全的占 14.5%，非常安全的占 26.6%。漏洞风险等级中，高危漏洞占比 19.5%，中危漏洞占比 65.6%，低危漏洞占比 15%。





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。截止 2 月 28 日，275 个系统整改完毕，通过复测，剩余 200 个存在高危漏洞风险的系统正在整改。

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。