2023 年网络与信息系统安全月报
（1-2 月）

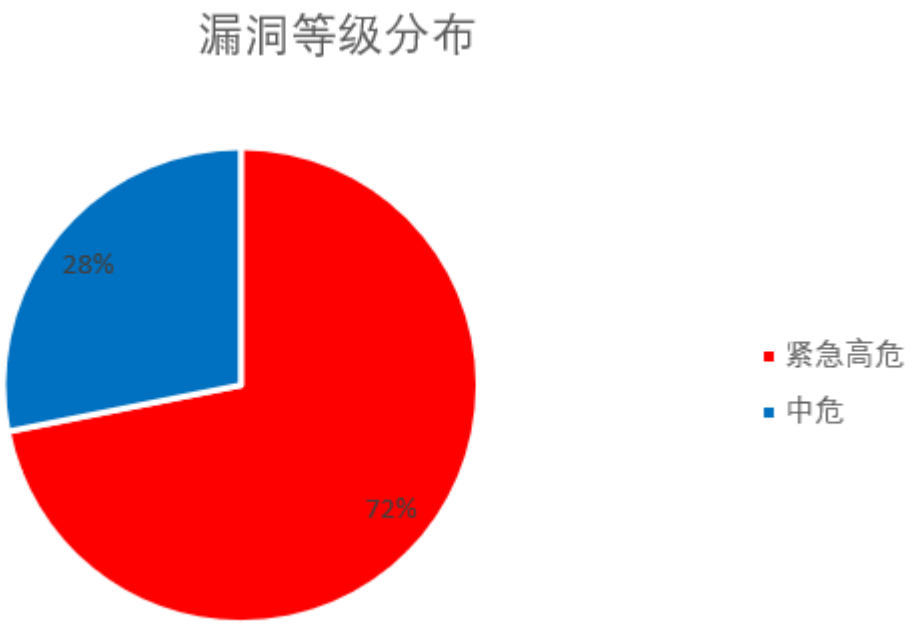
各单位、各部门：

为进一步加强校园网络安全管理，保障校园网络安全，现将1-2 月份网络与信息系统安全通报如下：

一、本月整体安全情况

(一)漏洞发现情况

1-2 月共发现漏洞 32 个。通过在校内网站监测、人工挖掘以及安全专项检查测试共发现漏洞 31 个，校外通报漏洞 1 个。其中紧急高危 23 个，中危漏洞 9 个，低危漏洞 0 个，紧急高危占比：72%。紧急、高危、中危、低危漏洞统计情况见下图：



注：

紧急高危漏洞是指可远程利用并能直接获取系统权限（服务器端权限、客户端权限）或者能够导致严重级别的信息泄漏（泄漏大量用户信息或学校机密信息）的漏洞，包括但不仅限于：命令注入、远程命令执行、上传获取 WebShell、SQL 注入、缓冲区溢出、绕过认证直接访问管理后台、核心业务非授权访问、核心业务后台弱密码等。

中危漏洞是指能直接盗取用户身份信息或者能够导致普通级别的信息泄漏的漏洞，包括但不限于目录浏览、客户端明文密码存储等。

低危漏洞是指能够导致轻微信息泄露的安全漏洞，包括但不仅限于 web 页面错误、堆栈信息泄露、JSONHijacking、CSRF、路径信息泄露、SVN 信息泄露、phpinfo 等。

(二)第三方漏洞通报

1-2 月所有漏洞通报均在规定时间内完成处理，未造成网络安全事件。

漏洞通报的来源包括：教育 SRC。

通报来源	网站（IP 地址）	漏洞类型	修复状态	部门
教育 SRC	http://jfpt.njtech.edu.cn	越权访问	已修复	计划财务处

(三)非法外链情况

1-2 月检查到 12 家单位所属网站共出现 13 次非法外链，具体情况如下：

网站（系统）	部门	频次	来源
http://kyy.njtech.edu.cn/	科学研究院	1 次	校内自查
http://trans.njtech.edu.cn	交通运输工程学院	1 次	校内自

			查
http://zwc.njtech.edu.cn/	后勤保障处	1 次	校内自查
http://tyxy.njtech.edu.cn/	体育学院	1 次	校内自查
http://jkjy.njtech.edu.cn/	后勤保障处	1 次	校内自查
http://mce.njtech.edu.cn/	材料化学工程国家重点实验室	2 次	校内自查
http://ny.njtech.edu.cn/	能源科学与工程学院	1 次	校内自查
http://tzb.njtech.edu.cn/	党委统战部	1 次	校内自查
http://jjc.njtech.edu.cn/	基本建设处	1 次	校内自查
http://jwc.njtech.edu.cn/	教务处	1 次	校内自查
http://lib.njtech.edu.cn/	图书馆	1 次	校内自查
http://life-phar.njtech.edu.cn/	生物与制药工程学	1 次	校内自

	院		查
https://alumni.njtech.edu.cn/	对外合作与发展处	1 次	通信管理局

(四)挖矿病毒

1-2 月重点针对我校挖矿病毒进行专项整治,期间共处理 92 起挖矿病毒事件，梳理矿池地址 19 个，并将矿池地址加入防火墙黑名单，及时阻断相关感染设备与校园网的连接，保障校园网络与信息系统安全。

本次专项整治未发现对外网提供应用服务的设备感染挖矿病毒的情况，所有感染挖矿病毒的电脑均为校园网内网设备，所涉及感染病毒的设备被及时阻断访问，具体名单如下：

IP 地址	所属部门
10.13.29.*	化学与分子工程学院
10.13.28.*	化学与分子工程学院
10.13.120.*	计算机科学与技术学院
10.25.24.*	土木工程学院
10.13.116.*	机械与动力工程学院
10.3.11.*	教务处

我校通过监测，多个存在挖矿病毒电脑回连到矿池 8999、5555、3333 等特殊端口，运维人员在日常巡检中应重点关注自身系统对外访问情况。

挖矿病毒危害：

1．主机长时间执行高性能计算，大量占用网络带宽、CPU及内存资源，不能及时处理用户的正常任务请求，造成主机响应速度明显减慢。

2. 中毒机器产生的能源消耗和碳排放量明显增大,同时加速CPU、内存等硬件老化速度。

3. 黑客通过挖矿程序窃取机密信息，比如机密文件、关键资产的用户名和密码等，导致校园 IT 资产遭受更进一步的资产损失。

4. 黑客控制主机作为“肉鸡”攻击互联网上的其他单位，或者作为继续对学校业务系统区域渗透的跳板，产生更严重的网络安全攻击事件。

5. 以“挖矿”产生的虚拟货币会促使网络黑产升级，变相滋生了各种网络犯罪，如勒索病毒往往都和虚拟货币关联在一起，严重威胁着校园网络环境的安全。

挖矿病毒防范措施：

1．安装杀毒软件，更新病毒库，进行杀毒。

2. 避免使用弱密码,避免多个系统使用同一密码,养成定期修改密码的习惯。

3. 关闭 Windows 共享服务、远程桌面控制等不必要的服务。

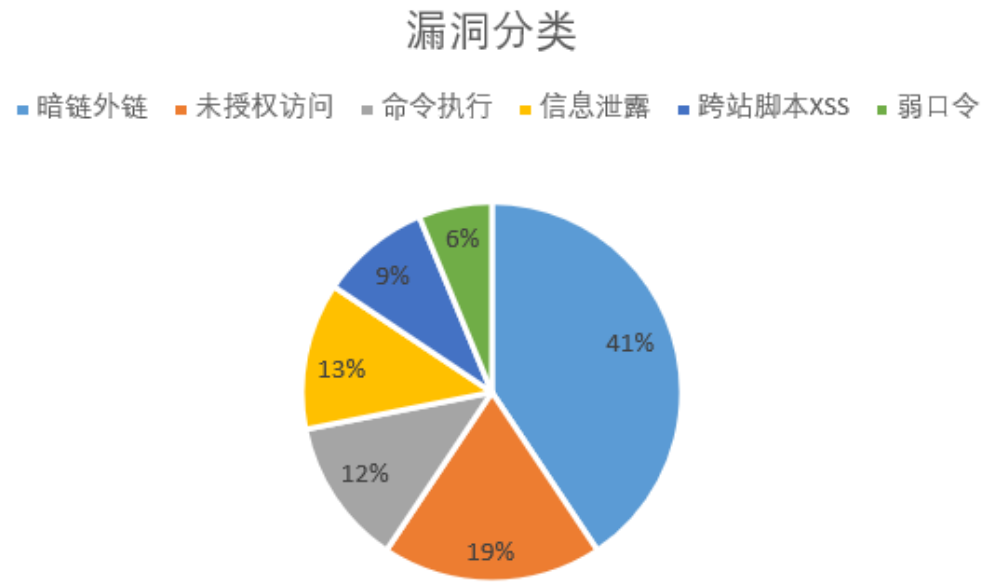
4. 不要安装不认识的、具有风险的应用；安装应用尽量到正规应用商店下载，使用学校正版化软件平台提供的软件。

5. 提高安全防范意识,不要随意插U盘,不要点击不明链接,不要打开邮件、微信等来历不明附件。

二、本月整体安全情况

(一)漏洞类型统计

1-2 月共发现信息系统漏洞 32 个。其中暗链外链 13 个，未授权访问 6 个，命令执行 4 个，信息泄露 4 个，跨站脚本 XSS3 个，弱口令 2 个。漏洞分类占比如下图：



(二)漏洞类型统计

1-2 月共发现漏洞 32 个，均已修复。

三、安全威胁风险与防范

安全威胁风险	防范措施建议
网站暗链外链较多	定期清理过期新闻公告，定期进行暗链外链扫描。
系统中间件版本过低导致命令执行	重要系统安装的中间件版本进行定期升级，扫描漏洞,。

系统存在弱口令情况	加强安全防范意识，定期更改口令，禁止使用弱密码。

四、网信安全每月小结

1-2月我校信息系统漏洞总数量较多，因各部门响应处理及时，未造成网络安全事件。1-2月网页暗链数量仍然较多，各部门需持续加强网页管理，及时清理过期信息。要督促系统运维商按时对信息系统进行巡检和维护，防止系统“带病”运行，危害网络安全。此外部分系统弱口令情况仍然存在，各部门需重点关注自建系统密码策略的严谨性。各部门要严格落实安全管理职责，摸清家底，精准施策，全流程掌握信息资产使用及管理维护状况，确保全校网络与信息系统持续安全稳定。

网络与信息系统安全联系电话：58139801。

信息管理中心

2023年3月6日