关于近期网络信息安全的预警提示

校内各部门:

据国家网络与信息安全信息通报中心监测发现，1 月下旬至今，有境外黑客组织借新型肺炎话题对我政府部门和医疗机构等目标实施网络攻击，意在窃取邮箱账号密码等敏感信息、开展情报收集。经分析研判，攻击者使用仿冒的 QQ 和 163 域名进行钓鱼，诱骗受害者点击伪造的“QQ 邮箱中转站文档”下载链接，从而窃取受害者的邮箱账号和密码，诱饵文档包括“基层党组织和党员防控疫情重大事项日报表”、“《南部杜氏中医》献方”等。在此基础上，攻击者可对相关机构开展进一步渗透入侵，目前已发现部分单位遭受攻击。

另有境外组织扬言对我国视频监控系统实施网络攻击破坏活动，为 2 月 13 日某纪念日预热。同时有“匿名者”黑客声称已掌握我境内大量摄像头监控权限。

鉴于上述黑客组织攻击活动指向明确、手法专业，请各部门高度重视，立即开展以下工作：

一是加强网络安全意识宣传，不要点击未知网站链接，切勿打开不明来历的邮件、文档。

二是做好资产清点盘查，加强网络安全管理。做好网站及网络设备安全管理，特别是视频监控系统，关闭不必要的网络服务和端口，系统设置强密码，加强登录审计和认证，降低入侵风险。

三是做好漏洞修复管理，及时消除安全隐患。及时跟进在用设备补丁更新情况，实时检测并修复系统安全漏洞，及时更新厂商发布的最新 rom。针对视频监控系统排查弱口令漏洞、后门漏洞、未授权访问漏洞、登录绕过漏洞等风险，并对境外黑客已声称探测的 CVE-2019-0708(Windows 远程桌面服务远程代码执行漏洞)、CVE-2009-3103(Windows 畸形 SMB 报文远程拒绝服务漏洞)等漏洞进行重点关注，加强边界管理防护。

四是全面落实值班值守制度，做好应急处置准备，发现网络攻击情况要迅速处置并及时报告。

联系人：姚嘉鑫　18980462002

信息中心

2020 年 2 月 11 日