中共安徽科技学院委员会网络安全与信息化办公室

网信〔2023〕28号

关于开展木马和僵尸网络安全专项治理工作的通知

各学院党委、机关党委、各党总支，各单位，各部门：

为了进一步贯彻落实党和国家关于网络安全工作的总体部署，有效遏制利用木马、僵尸网络发起大规模网络攻击的威胁，降低网络风险，学校网络与信息技术中心和各部门共同组织开展僵尸木马等网络安全专项治理工作，现将有关事项通知如下：

一、专项治理工作时间

通知发布之日起至年底。

二、工作阶段

1、10月23日-27日，安徽省教育厅组织开展2023年度网络安全攻防演练，组织攻击队伍，采取攻击源、攻击目标、攻击手段不明确的方式，对学校网站及相关信息系统展开攻击。

2、10月24日-29日，各单位（部门）专项处置活动动员，

按照网络安全防范工作提醒进行处置，开展网络防范的知识宣传教育引导。

3、10 月 30 日-11 月 3 日，开展学校网络安全应急演练和培训，通过漏洞挖掘或模拟，以学校某重要信息系统为重点进行应急演练。

4、网络与信息技术中心通过技术手段进行专项查杀，包括但不限于 xred 蠕虫、Tiggre 木马、NrsMiner 挖矿、Citeary 蠕虫等病毒。持续开展监测和处置，并根据上级部门监测通报的病毒情况，及时向有关单位发放网络安全处置通报，请收到通报的单位按时限要求整改处置，未及时进行处置的将对其账号或中病毒设备予以封禁，由此造成的工作影响，自行负责。

5、请各单位（部门）切实履行网络安全责任，做好所属信息系统的安全防护，跟进引导所辖人员网络安全隐患排除，各单位（部门）网络安全联络员做好本单位网站和信息系统的运行状况监测，保持通讯畅通，及时配合网络与信息技术中心进行通报和突发事件处置。

三、网络安全防范工作提醒

1、各单位（部门）对所管理信息系统开展全面自查，及时删除未实名登记、长期未使用的账号，特别注意并及时更改高权限管理账号、测试账号的弱口令。

2、严格管理个人上网认证账号，切勿借与他人使用，以免

造成网络安全责任不清。

3、计算机安装使用正版操作系统，打开系统自动更新功能，并及时安装系统补丁。（正版操作系统请到学校正版软件服务平台下载，http://ms.ahstu.edu.cn/）。凡是使用 Windows XP 操作系统的电脑终端一律升级到 Windows 7 以上版本。

4、计算机必须安装杀毒软件且升级至最新病毒库，定期进行全盘病毒查杀。对普通计算机，可安装“火绒”等免费杀毒软件，进行查杀。火绒下载：https://www.huorong.cn/。

5、关闭计算机设备上不必要的端口及服务，如 135，137，139，445，3389 等。

6、计算机登录密码要有足够的长度和复杂性，并定期更换登录密码。

7、提高网络安全防范意识，不打开来历不明的邮件附件、QQ 或微信文件，不浏览来历不明的网页，不随意点开来历不明链接，不下载安装来历不明的软件，不使用未经杀毒的 U 盘、移动硬盘等存储设备。

8、发现计算机使用异常，如突然出现卡顿、运行缓慢、上网异常等现象，请及时进行病毒查杀。对于检测出的异常结果无法确认是否为“挖矿”木马或者杀毒软件不能清除的情况，可联系网络与信息技术中心咨询。

专项治理期间，各单位（部门）发现任何问题或异常情况，

请及时联系网络与信息技术中心。联系人：李原，15005507202。

注：木马是指由攻击者安装在受害者计算机上秘密运行并用于窃取信息及远程控制的程序。僵尸网络是指由攻击者通过控制服务器控制的受害计算机群。现在两者有不断融合的趋势。通过木马和僵尸网络，黑客可以窃取个人隐私、散发垃圾邮件、发动分布式拒绝服务攻击正常的网站和系统。现在已经形成了巨大的黑色产业链，对互联网用户、政府机关、企事业单位、国家安全都是极大的隐患。

党委网信办

2023年10月24日

中共安徽科技学院委员会网络安全与信息化办公室　　2023年10月24日印发