

# 中共陕西省委教育工作委员会办公室

## 关于做好信息系统安全管理暨勒索病毒 防范工作的通知

各市教育局，杨凌示范区教育局、西咸新区教育卫体局，韩城市、神木市、府谷县教育局，各高等学校，委、厅各直属单位，直属中职学校：

近期，我省发生多起信息系统遭勒索病毒攻击事件，根据省委网信办相关要求，为加强我省教育领域信息系统安全管理，做好勒索病毒的防范工作，确保信息系统和网站稳定运行，现将有关事项及要求通知如下：

### 一、明确机构，责任到人

各级教育局、各学校和单位要加强网络信息安全组织机构建设，整合技术力量，确保有机构、有专人负责网络信息安全保障工作，责任落实到人。

### 二、全面排查，整改加固

各级教育局、各学校和单位要加强防范意识，加大防范力度，近期要组织技术力量，对信息系统和重点网站开展全面的安全漏洞监测，恶意代码和病毒查杀等工作，对于排查检测中发现的安全隐患和漏洞，要及时进行整改加固，全面提升抵御攻击、窃密

和非法控制的能力和水平。

各单位要重点做好防范勒索病毒感染工作，按省委网信办制定的《勒索病毒防范处置手册》（见附件）要求，认真查杀病毒、加强密码管理、及时备份数据，切实做好对勒索病毒的防范和处置工作。

### 三、监测预防，确保安全

各单位要通过人工和技术手段实现信息系统监测、预警，随时掌握信息系统和重点网站的运行状况及保障情况，确保发生网络安全事件时能够第一时间妥善快速处置。发生重大网络安全事件和勒索病毒攻击要及时上报省教育厅信息和学校保障工作处。

### 四、其他工作

1. 各市（区）教育局要将工作要求传达到辖区所有县（区）教育局和学校，保证工作落实到位。

2. 各高校、直属中职学校、各直属单位，要按照工作要求，尽快落实，确保信息系统安全。

联系人：侯瑞亮 029-88668695

中共陕西省委教育工委办公室



陕西省教育厅办公室

2018年12月26日





## 勒索病毒防范处置手册

### 一、勒索病毒介绍

勒索病毒，是一种新型电脑病毒，主要以邮件、程序木马、网页挂马的形式进行传播。该病毒性质恶劣、危害极大，一旦感染将给用户带来无法估量的损失。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。

一般情况下，勒索病毒文件一旦进入本地，就会自动运行，同时删除勒索软件样本，以躲避查杀和分析。接下来，勒索病毒利用本地的互联网访问权限连接至黑客的 C&C 服务器，进而上传本机信息并下载加密私钥与公钥，利用私钥和公钥对文件进行加密。除了病毒开发者本人，其他人是几乎不可能解密。加密完成后，还会修改壁纸，在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。且变种类型非常快，对常规的杀毒软件都具有免疫性。攻击的样本以 exe、js、wsf、vbe 等类型为主，常规依靠特征检测的安全产品对防范勒索病毒的没有有效办法。

### 二、病毒传播方式

勒索病毒主要通过以下三种途径传播：

一是通过系统漏洞进行传播。这种传播方式占到了总数的大部分。由于 win7、xp 等系统存在大量无法及时修复的漏洞，而

政府、企业、学校、医院等局域网机构用户使用较多的恰恰是 win7、xp 等系统，因此也成为病毒攻击的重灾区，病毒可以通过漏洞在局域网中无限传播。

二是通过邮件与广告推广进行传播。这种传播方式虽然占比不高，但对于有收发邮件、网页浏览需求的单位而言，依旧会受到威胁，并且按照 CNCERT 监测数据发现，邮件与广告钓鱼攻击不但是勒索病毒的传播途径，也是 APT 攻击的一个重要传播途径。

三是通过接入外部设备进行传播。对于某些特别依赖 U 盘、记录仪等外部设备办公的局域网用户来说，外部设备则成为勒索病毒攻击的特殊途径。对于大量的关键信息系统来说，很大一部分都是内网系统，非法的外部设备连接往往是这样的系统遭到攻击的最主要或者唯一途径。

### 三、防范措施

如何应对勒索病毒大量传播，主要有以下几项防范措施：

1. 及时备份重要文件，且文件备份应与主机隔离。
2. 及时安装更新补丁，避免一些勒索软件利用漏洞感染计算机。
3. 尽量避免打开社交媒体分享等来源不明的链接，给信任网站添加书签并通过书签访问；不要浏览来历不明的色情、赌博等网站，这些网站常常作为恶意代码放马地址。
4. 对非可信来源的邮件保持警惕，避免打开附件或点击邮件中的链接；不要轻易点开 js、vbs、bat、src、exe 等后缀名的文件。



5. 安装杀毒软件并及时更新病毒库，定期用杀毒软件扫描系统，如杀毒软件有启发式扫描功能，可使用该功能扫描计算机。

6. 部分勒索软件变种利用 RDP（远程桌面协议）暴力破解远端机器的密码实现传播。建议更换 RDP 服务端口号或关闭 RDP；关闭系统中不必要的端口，如 445、139、3389 等。

7. 检查并修改计算机上的弱密码；强制使用高强度密码策略；针对不同机器，选用不同的管理密码。

8. 建议服务器终端开启日志记录功能或增加集中日志审计措施，为追踪溯源提供基础。

9. 对于监管部门和行业主管部门来说，应加强宣传教育，向广大网民宣传勒索软件传播原理、危害、防护方法。

#### 四、处置建议

1. 不建议被病毒攻击的企业或者单位自行支付赎金，很多情况下，即使支付赎金，也很难找回被加密的数据文件。反而有可能受到更多的财产损失。

2. 隔离感染主机，通过关机、断网或修改访问控制策略的方式实现对于感染主机的物理隔离。

3. 针对重要服务器的数据备份，定期保存离线副本，利用备份数据还原系统，并确认还原后系统安全方可继续使用。

4. 向专业机构请求帮助，看是否有解密工具或者防范工具，一般情况下，现有的勒索软件都无法解密，只能通过防范措施，避免勒索病毒的进一步危害。