# **什么是勒索病毒？有哪些危害？如何预防？**

勒索病毒是泛指一切通过锁定被感染者计算机系统或文件并施以敲诈勒索的新型计算机病毒，通过计算机漏洞、邮件投递、恶意木马程序、网页后门等方式进行传播，一旦感染，磁盘上几乎所有格式的文件都会被加密，造成企业、学校和个人用户大量重要文件无法使用甚至外泄，严重影响日常工作和生活。

一般被勒索病毒感染后，将导致重要文件无法读取、关键数据被损坏、计算机被锁死无法正常使用等情况；为了指引被感染者缴纳赎金，勒索病毒还会在桌面等明显位置生成勒索提示文件，被感染者需要通过缴纳高额赎金才能获取解密密钥恢复计算机系统和数据文件的正常使用，****多数情况即使缴纳了高额的赎金也未必能正常恢复数据****。因此，勒索病毒具有数据恢复代价大和数据恢复可能性极低的特点。

****常见勒索病毒传播途径：****

****1.网站挂马****。用户浏览挂有木马病毒的网站，上网终端计算机系统极可能被植入木马并感染上勒索病毒。

****2.邮件传播****。邮件传播是目前互联网上常见的病毒传播方式。攻击者通过利用当前热门字样，在互联网上撒网式发送垃圾邮件、钓鱼邮件，一旦收件人点开带有勒索病毒的链接或附件，勒索病毒就会在计算机后台静默运行，实施勒索。

****3.漏洞传播****。通过计算机操作系统和应用软件的漏洞攻击并植入病毒是近年来流行的病毒传播方式。最典型的案例是2017年在国内泛滥的WannaCry大规模勒索事件，攻击者正是利用微软445端口协议漏洞，进行感染传播网内计算机。

****4.捆绑传播****。攻击者将勒索病毒与其他软件尤其是盗版软件、非法破解软件、激活工具进行捆绑，从而诱导用户点击下载安装，并随着宿主文件的捆绑安装进而感染用户的计算机系统。

****5.介质传播****。攻击者通过提前植入或通过交叉使用感染等方式将携有勒索病毒的U盘、光盘等介质进行勒索病毒的移动式传播。此种传播途径往往发生在文印店、公共办公区域等高频交叉使用可移动存储介质的场所，也可能通过广告活动派发、街区丢弃等方式实现诱导用户使用携带勒索病毒的U盘、光盘。携带勒索病毒的光盘、U盘一旦接入计算机，勒索病毒即可能随着其自动运行或用户点击运行导致计算机被感染。

****预防，是对付勒索病毒最为有效的手段！****

****防护建议：****

1.定期做好重要数据、文件的备份工作；

2.及时更新升级操作系统和应用软件，修复存在的中高危漏洞；

3.安装正版杀毒软件并及时升级病毒库，定期进行全面病毒扫描查杀；

4.在系统中禁用U盘、移动硬盘、光盘的自动运行功能，不要使用/打开来路不明的U盘、光盘、电子邮件、网址链接、文件；

5.避免使用弱口令，为每台服务器和终端设置不同口令，且采用大小写字母、数字、特殊字符混合的高复杂度组合结构，口令位数应8位以上；

6.不要在网上下载安装盗版软件、非法破解软件以及激活工具。