勒索软件防范指南

国家计算机网络应急技术处理协调中心

2021 年 7 月

勒索软件是黑客用来劫持用户资产或资源实施勒索的一种恶意程序。黑客利用勒索软件，通过加密用户数据、更改配**骆**等方式，使用户资产或资源无法正常使用，并以此为条件要求用户支付费用以获得解密密码或者恢复系统正常运行。主要的勒索形式包括文件加密勒索、锁屏勒索、系统锁定勒索和数据泄漏勒索等。主要的传播方式包括钓鱼邮件传播、网页挂马传播、漏洞传播、远程登录入侵传播、供应链传播和移动介质传播等。国家互联网应急中心（CNCERT）近期发布的《2020 年我国互联网网络安全态势综述》显示，2020 年勒索软件持续活跃，全年捕获勒索软件 78.1 万余个，较 2019 年同比增长 6.8%。2021 年上半年，勒索软件攻击愈发频繁，发生多起重大事件，例如 3 月 20 日，台湾计算机制造商宏**碁**（Acer）遭 REvil 勒索软件攻击，被要求支付 5000 万美元赎金；5 月 7 日，美国输油管道公司 Colonial Pipeline 遭 Darkside 勒索软件攻击，导致东海岸液体燃料停止运营；5 月 26 日，国内某大型地产公司遭 REvil 勒索软件攻击，窃取并加密了约 3TB 的数据；5 月 31 日，全球最大的肉类供应商 JBS 遭 REvil 勒索软件攻击，导致澳大利亚所有 JBS 肉类工厂停产。

一、勒索软件防范九要、四不要

防范勒索软件要做到以下“九要”：

1、要做好资产梳理与分级分类管理。清点和梳理组织内的信息

系统和应用程序，建立完整的资产清单；梳理通信数据在不同信息系统或设备间的流动方向，摸清攻击者横向移动可能路径；识别内部系统与外部第三方系统间的连接关系，尤其是与合作伙伴共享控制的区域，降低勒索软件从第三方系统进入的风险；对信息系统、数据进行分级分类，识别关键业务和关键系统，识别关键业务和关键系统间的依赖关系，确定应急响应的优先级。

2、要备份重要数据和系统。重要的文件、数据和业务系统要定期进行备份，并采取隔离措施，严格限制对备份设备和备份数据的访问权限，防止勒索软件横移对备份数据进行加密。

3、要设置复杂密码并保密。使用高强度且无规律的登录密码，要求包括数字、大小写字母、符号，且长度至少为 8 位的密码，并经常更换密码；对于同一局域网内的设备杜绝使用同一密码，杜绝密码与设备信息（例如 IP、设备名）具有强关联性。

4、要定期安全风险评估。定期开展风险评估与渗透测试，识别并记录资产脆弱性，确定信息系统攻击面，及时修复系统存在的安全漏洞。

5、要常杀毒、关端口。安装杀毒软件并定期更新病毒库，定期全盘杀毒；关闭不必要的服务和端口，包括不必要的远程访问服务（3389 端口、22 端口），以及不必要的 135、139、445 等局域网共享端口等。

6、要做好身份验证和权限管理。加强访问凭证颁发、管理、验

证、撤销和审计，防止勒索软件非法获取和使用访问凭证，建议使用双因子身份认证；细化权限管理，遵守最小特权原则和职责分离原则，合理配**珞**访问权限和授权，尽量使用标准用户而非管理员权限用户。

7、要严格访问控制策略。加强网络隔离，使用网络分段、网络划分等技术实现不同信息设备间的网络隔离，禁止或限制网络内机器之间不必要的访问通道；严格远程访问管理，限制对重要数据或系统的访问，如无必要关闭所有远程管理端口，若必须开放远程管理端口，使用白名单策略结合防火墙、身份验证、行为审计等访问控制技术细化访问授权范围，定期梳理访问控制策略。

8、要提高人员安全意识。为组织内人员和合作伙伴提供网络安全意识教育;教育开发人员开发和测试环境要与生产环境分开，防止勒索软件从开发和测试系统传播到生产系统。

9、要制定应急响应预案。针对重要信息系统，制定勒索软件应急响应预案，明确应急人员与职责，制定信息系统应急和恢复方案，并定期开展演练；制定事件响应流程，必要时请专业安全司协助，分析清楚攻击入侵途径，并及时加固堵塞漏洞。

防范勒索软件要做到以下“四不要”：

1、不要点击来源不明邮件。勒索软件攻击者常常利用受害者关注的热点问题发送钓鱼邮件，甚至还会利用攻陷的受害者单位组织或熟人邮箱发送钓鱼邮件，不要点击此类邮件正文中的链接或

附件内容。如果收到了单位组织内或熟人的可疑邮件，可直接拨打电话向其核实。

2、不要打开来源不可靠网站。不浏览色情、赌博等不良信息网站，此类网站经常被勒索软件攻击者发起挂马、钓鱼等攻击。

3、不要安装来源不明软件。不要从不明网站下载安装软件，不要安装陌生人发送的软件,警惕勒索软件伪装为正常软件的更新升级。

4、不要插拔来历不明的存储介质。不要随意将来历不明的 U 盘、移动硬盘、闪存卡等移动存储设备插入机器。

二、勒索软件应急处置方法

当机器感染勒索软件后，不要惊慌，可立即开展以下应急工作，降低勒索软件产生的危害。

1、隔离网络。采用拔掉网线或者禁用网络等方式切断受感染机器的网络连接，避免网络内其他机器被进一步感染渗透。

2、分类处置。当发现机器上重要文件尚未被加密时，应立即终止勒索软件进程或者关闭机器，及时止损；当发现机器上重要文件已被全部加密时，可保持机器开机原状态，等待专业处置。

3、及时报告。及时报告网络管理员，通知其他可能会受到勒索软件影响的人员。造成重大影响时，及时向网络安全主管部门报告。

4、排查加固。立即视情况切断网络内机器间不必要的网络连接，

修改网络内机器的弱口令密码。全面排查勒索软件植入途径，并及时堵塞漏洞。尽快对网络内机器进行全面漏洞扫描与安全加固。

5、专业恢复。请专业公司和人员进行数据和系统恢复工作。

CNCERT 联系方式：010-82990999，cncert@cert.org.cn