勒索病毒防护

勒索病毒分类

NO.01 文件加密类勒索病毒

该类勒索病毒以RSA、AES等多种加密算法对用户文件进行加密，并以此索要赎金，一旦感染，极难恢复文件。

NO.02 数据窃取类勒索病毒

该类勒索病毒与文件加密类勒索病毒类似，但在勒索环节，攻击者通过甄别和窃取用户重要数据，以公开重要数据胁迫用户支付勒索赎金。

NO.03 系统加密类勒索病毒

该类勒索病毒同样通过各类加密算法对系统磁盘主引导记录、卷引导记录等进行加密，阻止用户访问磁盘，影响用户设备的正常启动和使用，并向用户勒索赎金。

NO.04 屏幕锁定类勒索病毒

该类勒索病毒对用户设备屏幕进行锁定，通常以全屏形式呈现涵盖勒索信息的图像，导致用户无法登录和使用设备，进而勒索赎金，但该类勒索病毒未对用户数据进行加密，具备数据恢复的可能。

勒索病毒传播方式

利用安全漏洞传播

攻击者利用弱口令、远程代码执行等网络产品安全漏洞，攻击入侵用户内部网络，获取管理员权限，进而主动传播勒索病毒。目前，攻击者通常利用已公开且已发布补丁的漏洞，通过扫描发现未及时修补漏洞的设备，利用漏洞攻击入侵并部署勒索病毒，实施勒索行为。

利用钓鱼邮件传播

攻击者将勒索病毒内嵌至钓鱼邮件的文档、图片等附件中，或将勒索病毒恶意链接写入钓鱼邮件正文中，通过网络钓鱼攻击传播勒索病毒。一旦用户打开邮件附件，或点击恶意链接，勒索病毒将自动加载、安装和运行，实现实施勒索病毒攻击的目的。

利用网站挂马传播

攻击者通过网络攻击网站，以在网站植入恶意代码的方式挂马，或通过主动搭建包含恶意代码的网站，诱导用户访问网站并触发恶意代码，劫持用户当前访问页面至勒索病毒下载链接并执行，进而向用户设备植入勒索病毒。

利用远程桌面入侵传播

攻击者通常利用弱口令、暴力破解等方式获取攻击目标服务器远程登录用户名和密码，进而通过远程桌面协议登录服务器并植入勒索病毒。同时，攻击者一旦成功登录服务器，获得服务器控制权限，可以服务器为攻击跳板，在用户内部网络进一步传播勒索病毒。

利用软件供应链传播

攻击者利用软件供应商与软件用户间的信任关系，通过攻击入侵软件供应商相关服务器设备，利用软件供应链分发、更新等机制，在合法软件正常传播、升级等过程中，对合法软件进行劫持或篡改，规避用户网络安全防护机制，传播勒索病毒。

利用移动介质传播

攻击者通过隐藏U盘、移动硬盘等移动存储介质原有文件，创建与移动存储介质盘符、图标等相同的快捷方式，一旦用户点击，自动运行勒索病毒。

内容来源：智慧通大