重庆市网络与信息安全信息通报中心

渝网通〔2019〕13号

关于做好“勒索病毒”安全防范工作的通知

各通报机制成员单位，各相关单位：

工作掌握，近期勒索病毒不断发生变种，病毒攻击传播呈现扩散势头，国内有多个省、市级重要单位遭受攻击，我市也有部分单位因勒索病毒攻击导致系统崩溃，少数单位因缺乏数据备份机制，导致数据丢失，造成严重后果。为切实做好“勒索病毒”安全防范工作，现将相关工作要求通知如下：

一、高度重视，认清形势

“勒索病毒”主要利用**系统安全漏洞、电子邮件、代码嵌入、网页挂马**等方式进行攻击植入，并通过网络中未升级补丁的**薄弱端口、移动存储介质**等自主复制、肆意传播，采用非对称加密算法对文件和数据库进行强加密，导致受感染主机服务中断、数据丢失，危害及其严重。通过对近期爆发的 GlobeImposter、GandCrab、Crysis 等多个勒索病毒版本进行分析，攻击者逐步将攻击的矛头对准电子政务、金融、卫生、医疗、水利等重点行业的关键信息基础设

施和重要信息系统，并随着新漏洞的爆发不断更换版本、扩展攻击途径，甚至通过勒索“赎金”形成黑色产业链，已成为党政机关、企事业单位面临的重大网络安全威胁之一。各单位要深刻认识到当前面临勒索病毒攻击的严峻形势，切实履行网络安全保护主体责任，按照“谁主管、谁负责，谁运营、谁负责”的原则，加强组织领导，结合本行业、本单位网络和系统运营使用情况研究防护应对措施，部署开展安全排查加固等工作，确保层层压实责任，网络、系统和终端安全防御全覆盖、不留死角。

二、落实防护措施，加强安全管理

各单位要从网络安全管理和技术防护措施两个方向发力，建立起有效抵御勒索病毒的“防火墙”。要严格机房人员、移动存储介质、运维保障、安全监测等管理制度的落实，对单位所有互联网、业务专网、内部局域网等环境、业务终端和信息系统（含暂停使用未下线的系统）等开展全面安全排查，发现安全问题隐患及时开展整改加固工作。在开展排查工作中，要重点落实以下防护措施。

（一）网络层防御。单位网络必须按照“最小化”原则对外开放连接，远程系统登录、桌面管理、文件传输等应采取“强账号+复杂密码+限制IP访问”等策略配置阻断外部网络嗅探、渗透攻击。单位网络要按照业务功能划分严格实行分区管理，对连接各分区的核心交换机、路由器等网络设备的账号权限、通信设置、安全配置、运行状态等开展检查复核，根据需求限制136、139、445等高危端口通信流量，挤压病毒传播空间，阻断病毒扩散路径，严防出现“单点突破、全网沦陷”被动局面。

（二）系统层防御。一是对单位运营的各业务信息系统安全开展全面排查，账号密码设置、系统开放端口、文件上传共享、后台管理模块、客户端输入等重点部位应逐项清理，坚决杜绝默认账号弱口令、SQL 注入、XSS 跨站、任意文件上传、越权访问等高危漏洞。**二是**业务系统运行所依托的 Struts2、OpenSSL、Jboss、Weblogic、Java 库、DBMS 数据库管理系统等第三方环境应根据官方信息升级最新补丁，且设定账号应与操作系统账号严格分离、降权使用。**三是**各业务系统运行的操作系统环境宜采用较高版本，且按照操作系统官方公告及时升级更新、完善补丁，堵塞 WannaCry、SMB 远程溢出等高危漏洞。

（三）主机层防御。单位服务器和应用终端应实行专人管理、专机专用，要安装并启用病毒查杀、流量监测、防火墙等安全软件，及时更新病毒库，定时扫描检测。要关闭不必要的远程访问端口（如 21、22、445、139、3389 等），落实安全审计技术措施，做好日志记录留存。尤其要强化对移动硬盘、U 盘、光盘等移动存储介质的管理和使用，专网专用、先杀后用，防止成为病毒的“扩散摆渡”载体。

（四）意识层防御。要组织单位员工开展宣传和教育培训，建立网络安全思想层“防火墙”。必须严格遵守单位网络安全管理的各项规章制度，做到安全用网，杜绝因贪图方便出现违规外联、移动存储介质混用、弱口令使用等威胁网络安全的情形。在使用单位网络开展日常工作中，应选用可信网络资源，不要访问风险网站；不要点击陌生 Email 携带的任何附件、URL；不要下载安装可疑程

序等，防止遭受网站挂马、恶意代码嵌入、病毒植入等网络攻击。

三、建立常态机制，有效应对处置

防范勒索病毒是一项长期、艰巨的任务，要站在做好网络安全工作的高度积极防御、有效应对。

（一）坚持常态化风险排查。各单位要结合日常网络安全运维工作，建立风险隐患常态化排查整改机制。组织网络安全管理部门、运维部门、技术机构等定期对单位网络、信息系统运行情况开展安全自查自纠，发现问题隐患形成清单、落实整改、做好记录，确保问题清零。

（二）严格落实数据备份工作。勒索病毒攻击的对象是加密绑架含文件文档、业务系统代码、数据库存储等在内的重要数据，**做好数据备份工作是防御、应对病毒攻击最有力的措施之一。**要定期对单位重要信息系统程序、文件和数据进行备份，尤其是采用线下或异地备份方式，确保数据安全。

（三）完善预案做好应对处置。各单位要将发生勒索病毒攻击事件应对处置流程纳入单位《网络安全事件应急处置工作预案》中进一步完善，储备应急资源、做好应急保障，确保遭受攻击能迅速采取断网、隔离等措施阻止病毒蔓延，同步启动预案开展病毒清除、数据恢复等处置工作，可通过启用备用系统、格式化后重装服务器、加载备份程序、数据等方式恢复系统正常运营。重要信息系统遭受攻击应保护好现场，第一时间向同级公安机关报告并协助开展案（事）件调查工作。

联系人：杜建军、郭金全，联系电话：63757224、63757213

重庆市网络与信息安全信息通报中心

2019年5月27日