贵州省教育厅办公室

省教育厅办公室关于应对最新变种“勒索病毒”的预警通报

各市（州）教育局，贵安新区社会事务管理局，各县（市、区、特区）教育局，各高等学校，省属中职学校，厅属高中，厅各处室（单位）：

近日，国内部分单位、医院的服务器被最新变种的“勒索病毒”攻击，导致服务器系统大面积瘫痪，造成不良影响。此次攻击与去年不同的是，去年“永恒之蓝”勒索病毒采用大面积撒网的方式进行传播。本次变种“勒索病毒”采取点对点人工渗透的方式进行攻击，首先有针对性的利用远程桌面漏洞、弱口令等安全漏洞攻破某个单位网络主机，再利用该主机扫描全网内未修补补丁的系统和主机，一旦发现存在勒索病毒漏洞，则植入木马进行破坏。较去年而言，此次攻击更具针对性，造成影响更恶劣。

一、病毒基本情况

此次传播的病毒是Globelmposter2.0病毒家族的其中一种后缀格式，其他后缀格式还有.GOTHAM;.CHAK;.GRANNY;.SKUNK;.TRUE;.SEXY;.MAKGR;.BIGI;.LIN;.BIIT;.reserve;.BUNNY;,FREEMAN。勒索通知信息文件为how_to_back_files.html。此病毒通过RDP远程桌面入侵桌面入侵施放病毒，病毒会加密本地磁盘与共享

文件夹的所有文件。

二、防护措施

为降低“勒索病毒”可能造成的不良影响，建议从以下6各方面开展安全防护工作：

（一）提升新兴威胁对抗能力。从安全的技术、管理和运营等多个维度出发，对单位的互联网边界、防御体系及安全运营制度等多方面进行加强；在网络边界、终端部署基础防护设备，增加实时感知威胁攻击和持续响应的能力；

（二）周期性对单位网络进行安全评估工作，及时发现网络主机存在的安全缺陷，修复高风险漏洞；

（三）及时给办公终端和服务器打补丁修复漏洞，包括操作系统及第三方应用的补丁；

（四）尽量关闭不必要的常见网络端口，例如：445、3389等；

（五）修改办公系统或服务器登录密码，并定期更换密码；

（六）对重要数据和文件及时进行备份，提高安全运维人员职业素养，定期对电脑、移动存储介质进行木马病毒查杀。

三、处置建议

如发现系统已经感染病毒，可从以下5个方面开展工作：

（一）断开网络，预防感染计算机其他文件；

（二）结束病毒进程，安装杀毒软件，查杀病毒，预防二次中毒；

（三）备份加密数据。预防意外造成加密数据损害无法解密；

（四）排查服务器的局域网是否有共享文件夹文件被加

密，备份他们；

（五）报告属地网信办，寻求技术支撑。

四、工作要求

目前正值全国“两会”召开的敏感时期，为全力保障“两会”期间网络安全，要高度重视，及时警示本部门、本地网站和系统用户，关注各厂商发布的漏洞修复措施，使用前做好补丁验证、系统备份等工作，在确保安全的前提下及时堵塞漏洞，消除安全隐患，提高安全防范能力，发现系统遭攻击情况后及时报告省教育管理信息中心。（联系人：杨燕；联系电话：0851-85283616 ；联系邮箱：gzjyglxxzx@sina.com）

省教育厅办公室

2018年3月1日