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

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