网络与信息安全情况通报

第 7 期

深圳市网络与信息安全信息通报中心　　2017 年 5 月 13 日

关于加强对 wana 新型勒索病毒防范工作的紧急通知

我中心在工作中掌握,近期一种 wana 新型恶意软件(病毒)爆发传播。该恶意软件为勒索软件，利用 NSA 泄露的黑客武器攻击 Windows 漏洞进行快速传播。一旦系统中毒后，文件资料会立即被加密,需要向软件制作者缴纳一定数量的电子货币(比特币）才能解密恢复。为确保我市各重要信息系统安全稳定运行，维护“一路一带”峰会、文博会举办期间稳定秩序，请各重点单位立即开展安全加固工作。现将具体情况通知如下：

一、病毒传播机理

本次爆发的勒索病毒是利用 NSA 泄露的一款“永恒之蓝”黑客软件武器进行传播。永恒之蓝”将远程扫描并攻击 Windows 系统的 445 端口（文件共享端口），用户无需做任何操作，黑

客就可通过 445 端口利用 SMB 系统服务漏洞，进而执行任意代码和植入恶意程序。

二、防范建议和措施

一是更新最新的操作系统补丁，确保已安装微软于今年 3 月份发布的该漏洞补丁（相关说明见：https://technet.microsoft.com/zh-cn/library/security/ms17-010.aspx）。

二是关闭操作系统不必要开放的端口如 445、135、137、138、139 等，关闭网络共享功能。

三是对重要文件数据严格进行定期备份。

请各单位立即组织技术力量开展安全加固工作，彻底排除漏洞隐患，确保信息系统安全稳定运行。一旦发现系统中毒被勒索赎金的情况，第一时间上报我中心（电话：84452816）。

深圳市网络与信息安全

信息通报中心

2017 年 5 月 13 日

报：国家网络与信息安全信息通报中心；

省公安厅网警总队；

市委办公厅、市人大常委会办公厅、市政府办公厅、市政协办公厅。

送：各有关单位。

发：市公安局各分局。

（共印 120 份，存档 1 份）