政 务

湖北省互联网信息办公室

关于做好“必加”勒索软件防范应对工作的通知

各地各单位:

近日，多个国家遭受“必加（Petya）”勒索软件攻击，影响多处重要基础设施，我境内也开始有用户受到影响。

为做好防范应对工作，避免造成不良影响，请各单位按照国家网络安全事件应急预案，采取阻断隔离措施。一旦发生被勒索软件感染事件，立即做好应急处置，并向省网络安全与信息化领导小组办公室报告情况。请省直各单位及中央在汉企事业单位于7月4日15:00前将排查数据统计情况（附件1）通过电子政务内网安全邮件反馈至我办（省委宣传部-网络安全与技术处-杨青亮）。请各地网信办组织做好本地防范工作，于7月4日15时前完成本地数据统计，并通过RTX上报至省网信办-网络安全与技术处。

联系人：杨青亮 027-87813974

附件：1.排查防范情况统计表

2.“必加”勒索软件排查防范措施（供参考）

湖北省互联网信息办公室

2017年6月30日

附件 1

排查防范情况统计表

终端			
排查终端总数			
受感染终端总数			
其中	Windows 7	数量	
	Windows 8	数量	
	Windows 8.1	数量	
	Windows 10	数量	
	WindowsXP	数量	
	WindowsVista	数量	
	其他	数量	
服务器			
排查服务器总数			
受感染服务器总数			
其中	WindowsServer 2003	数量	
	WindowsServer 2008	数量	
	WindowsServer 2012	数量	
	WindowsServer 2016	数量	
	其他	数量	

排查应包含虚拟主机

附件 2

“必加”勒索软件排查防范措施（供参考）

1. 更新防病毒产品病毒库。

2. 对 Windows 操作系统口令进行排查，杜绝使用空口令、弱口令、相同口令、长期未更新口令。修改网络管理员主机密码和域控密码，并避免在非域控服务器上使用域控管理员权限登陆。

3. 提醒工作人员不要轻易点击来源不明邮件中的链接、附件等，尤其是 rtf、doc 等格式文件。

4. 对使用 windows 操作系统的终端和服务器，更新微软针对“永恒之蓝”、“永恒浪漫”发布的系统补丁。

5. 无法采取自动更新措施的，可至微软官方网站下载补丁后手动更新。补丁下载地址：https://technet.microsoft.com/zh-cn/library/security/4025685

6. 确实无法及时更新补丁的，可选择采取以下 1 项或 2 项临时措施：

（1）禁用 Windows 操作系统的 SMBv1 服务，步骤可参考：https://support.microsoft.com/zh-cn/help/2696547/how

-to-enbale-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows

（2）在本地网络路由器或防火墙上屏蔽对445端口的访问。

5.在不影响正式使用和服务的前提下，可以进一步采取以下1项或多项临时措施：

（1）关闭终端和服务器的远程文件共享。

（2）停止 Windows 操作系统的 WMI（Windows Management Instrumentation Windows）服务。

（3）在本地网络路由器或防火墙上屏蔽对139和445端口的访问。

6.在网络流量监测设备中配置监测策略，提高发现病毒传播能力。持续关注有关部门发布的风险提示、通报、预警信息，及时采取进一步对应措施。