常州市网络与信息安全协调小组办公室文件

常信安办〔2017〕9号

关于防范 EternalRocks 蠕虫病毒的通知

各辖市、区人民政府，市各委办局，市各公司、直属单位：

北京时间 5 月 17 日晚，安全专家发现了一种基于类似 WannaCry 的蠕虫病毒，也是通过 NSA 武器库中的漏洞进行传播，安全专家在对其进行分析之后发现，EternalRocks 具有病毒的特征，而且能够进行自我传播，其危害性需要引起各单位的高度重视。

Eternalrocks 由 7 个攻击载荷组成，包括 4 个 Windows 漏洞利用程序、1 个后门程序和 2 个漏洞扫描程序。4 个漏洞利用均利用了 Windows 系统 SMB 协议存在的漏洞，涉及 Windows XP, Vista, 7, Windows Server 2003, 2008, 2008 R2 系统。Eternalrocks 不会对感染主机的文件进行加密并

勒索比特币，但会在被感染的主机上安装 Doublepulsar 后门，此后门被黑客利用，可以远程控制被感染主机。

该漏洞影响所有开放 445 端口的未更新补丁的 windows 系统，包括工控机、终端机、PC 机、服务器等。据 2017 年 5 月 21 日报道，EternalRocks 影响了大量未安装补丁的 Windows7 主机，传播速度快，目前已经影响了 24 万主机。

请各地区、各部门、各单位高度重视该病毒情况，做好以下防御措施:

1、在网络边界，如防火墙和路由器设备中阻断 TCP 135、137、139、445 端口的连接请求;

2、开启 windowsupdate，将补丁升级到最新;

3、开启 Windows Defender 或其它防护软件;

4、对重要文档、资料进行备份。

常州市网络与信息安全协调小组办公室

2017 年 05 月 26 日