关于加强防范“暗云”木马程序的通知

根据国家互联网应急中心通报，一款名为“暗云”的木马在互联网大规模传播，我国境内已有大量用户感染，对我国互联网安全构成一定的威胁。目前该木马程序控制的主机已经组成一个超大规模的跨境僵尸网络，黑客不仅可以窃取我国百万计网民的个人隐私信息，而且一旦利用该僵尸网络发起 DDOS 攻击将对我国互联网稳定运行造成严重影响。为此，请各部门立即开展安全防范工作，具体情况通报如下：

1、“暗云”系列木马程序基本情况

“暗云”系列木马具有隐蔽性强、潜在危害大、传播范围广等特点。目前最新的变种“暗云Ⅲ”木马程序可在每次用户开机时从云端服务器下载并更新功能模块，可灵活变换攻击行为。2017 年 6 月 9 日至今，国家互联网应急中心监测发现我国境内有 160 余万台电脑感染了此木马。目前，该木马仅能感染 Windows 系统电脑。

2、木马排查和防范措施建议

（1）国家互联网应急中心开通了“暗云”木马感染数据免费查询服务，点击网址 http://d.cert.org.cn/即可查询使用的 IP 地址是否受到木马感染。

（2）不要选择安装捆绑在下载器中的软件，不要运行来源不明或被安全软件报警的程序，不要下载运行游戏外挂、私服登录器等软件。

（3）定期在不同的存储介质上备份信息系统业务和个人数据。

（4）下载主流杀毒软件进行检测和查杀。