工业和信息化部关于印发《公共互联网网络安全威胁监测与处置办法》的通知

工信部网安[2017]202号

各省、自治区、直辖市通信管理局，中国电信集团公司、中国移动通信集团公司、中国联合网络通信集团有限公司，国家计算机网络应急技术处理协调中心、中国信息通信研究院、国家工业信息安全发展研究中心、中国互联网协会，域名注册管理和服务机构、互联网企业、网络安全企业：

为深入贯彻习近平总书记关于网络安全的重要讲话精神，积极应对严峻复杂的网络安全形势，进一步健全公共互联网网络安全威胁监测与处置机制，维护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》等有关法律法规，制定《公共互联网网络安全威胁监测与处置办法》。现印发给你们，请结合实际，切实抓好贯彻落实。

工业和信息化部

2017年8月9日

公共互联网网络安全威胁监测与处置办法

第一条 为加强和规范公共互联网网络安全威胁监测与处置工作，消除安全隐患，制止攻击行为，避免危害发生，降低安全风险，维护网络秩序和公共利益，保护公民、法人和其他组织的合法权益，根据《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《中华人民共和国电信条例》等有关法律法规和工业和信息化部职责，制定本办法。

第二条 本办法所称公共互联网网络安全威胁是指公共互联网上存在或传播的、可能或已经对公众造成危害的网络资源、恶意程序、安全隐患或安全事件，包括：

（一）被用于实施网络攻击的恶意IP地址、恶意域名、恶意URL、恶意电子信息，包括木马和僵尸网络控制端，钓鱼网站，钓鱼电子邮件、短信/彩信、即时通信等；

（二）被用于实施网络攻击的恶意程序，包括木马、病毒、僵尸程序、移动恶意程序等；

（三）网络服务和产品中存在的安全隐患，包括硬件漏洞、代码漏洞、业务逻辑漏洞、弱口令、后门等；

（四）网络服务和产品已被非法入侵、非法控制的网络安全事件，包括主机受控、数据泄露、网页篡改等；

（五）其他威胁网络安全或存在安全隐患的情形。

第三条 工业和信息化部负责组织开展全国公共互联网网络安全威胁监测与处置工作。各省、自治区、直辖市通信管理局负责组织开展本行政区域内公共互联网网络安全威胁监测与处置工作。工业和信息化部 and 各省、自治区、直辖市通信管理局以下统称为电信主管部门。

第四条 网络安全威胁监测与处置工作坚持及时发现、科学认定、有效处置的原则。

第五条 相关专业机构、基础电信企业、网络安全企业、互联网企业、域名注册管理和服务机构等应当加强网络安全威胁监测与处置工作，明确责任部门、责任人和联系人，加强相关技术手段建设，不断提高网络安全威胁监测与处置的及时性、准确性和有效性。

第六条 相关专业机构、基础电信企业、网络安全企业、互联网企业、域名注册管理和服务机构等监测发现网络安全威胁后，属于本单位自身问题的，应当立即进行处置，涉及其他主体的，应当及时将有关信息按照规定的内容要素和格式提交至工业和信息化部和相关省、自治区、直辖市通信管理局。

工业和信息化部建立网络安全威胁信息共享平台，统一汇集、存储、分析、通报、发布网络安全威胁信息；制定相关接口规范，与相关单位网络安全监测平台实现对接。国家计算机网络应急技术处理协调中心负责平台建设和运行维护工作。

第七条 电信主管部门委托国家计算机网络应急技术处理协调中心、中国信息通信研究院等专业机构对相关单位提交的网络安全威胁信息进行认定，并提出处置建议。认定工作应当坚持科学严谨、公平公正、及时高效的原则。电信主管部门对参与认定工作的专业机构和人员加强管理与培训。

第八条 电信主管部门对专业机构的认定和处置意见进行审查后，可以对网络安全威胁采取以下一项或多项处置措施：

（一）通知基础电信企业、互联网企业、域名注册管理和服务机构等，由其对恶意 IP 地址（或宽带接入账号）、恶意域名、恶意 URL、恶意电子邮件账号或恶意手机号码等，采取停止服务或屏蔽等措施。

（二）通知网络服务提供者，由其清除本单位网络、系统或网站中存在的可能传播扩散的恶意程序。

（三）通知存在漏洞、后门或已经被非法入侵、控制、篡改的网络服务和产品的提供者，由其采取整改措施，消除安全隐患；对涉及党政机关和关键信息基础设施的，同时通报其上级主管单位和网信部门。

（四）其他可以消除、制止或控制网络安全威胁的技术措施。

电信主管部门的处置通知应当通过书面或可验证来源的电子方式等形式送达相关单位，紧急情况下，可先电话通知，后补书面通知。

第九条 基础电信企业、互联网企业、域名注册管理和服务机构等应当为电信主管部门依法查询 IP 地址归属、域名注册等信息提供技术支持和协助，并按照电信主管部门的通知和时限要求采取相应处置措施，反馈处置结果。负责网络安全威胁认定的专业机构应当对相关处置情况进行验证。

第十条 相关组织或个人对按照本办法第八条第（一）款采取的处置措施不服的，有权在 10 个工作日内向做出处置决定的电信主管部门进行申诉。相关电信主管部门接到申诉后应当及时组织核查，并在 30 个工作日内予以答复。

第十一条 鼓励相关单位以行业自律或技术合作、技术服务等形式开展网络安全威胁监测与处置工作，并对处置行为负责，监测与处置结果应当及时报送电信主管部门。

第十二条 基础电信企业、互联网企业、域名注册管理和服务机构等未按照电信主管部门通知要求采取网络安全威胁处置措施的，由电信主管部门依据《中华人民共和国网络安全法》第五十六条、第五十九条、第六十条、第六十八条等规定进行约谈或给予警告、罚款等行政处罚。

第十三条 造成或可能造成严重社会危害或影响的公共互联网网络安全突发事件的监测与处置工作，按照国家和电信主管部门有关应急预案执行。

第十四条 各省、自治区、直辖市通信管理局可参照本办法制定本行政区域网络安全威胁监测与处置办法实施细则。

第十五条 本办法自2018年1月1日起实施。2009年4月13日印发的《木马和僵尸网络监测与处置机制》和2011年12月9日印发的《移动互联网恶意程序监测与处置机制》同时废止。