网络信息安全周报

【2017】第 23 期

党委宣传部
信息网络中心 编

2017 年 9 月 28 日

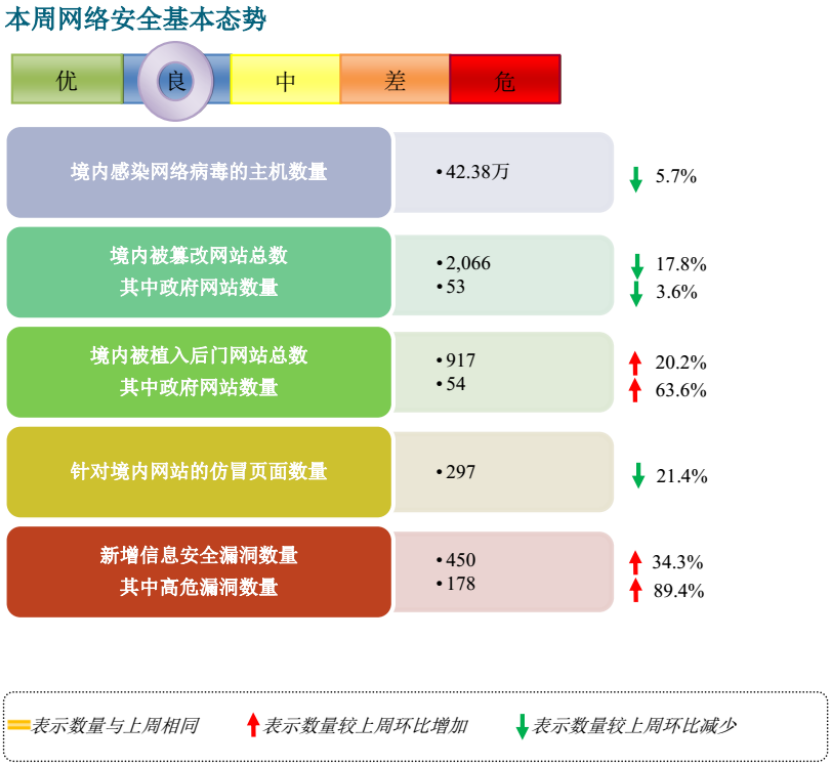
本期要目

- 【权威发布】全国网络安全信息与动态（2017 年 9 月 11 日—9 月 17 日）
- 【城院 IT】综合业务管理平台统计信息（2017 年 9 月 18 日—9 月 24 日）
- 【新闻速递】工信部发布《公共互联网网络安全威胁监测与处置办法》
- 【安全速递】《公共互联网网络安全威胁监测与处置办法》

全国网络安全信息与动态

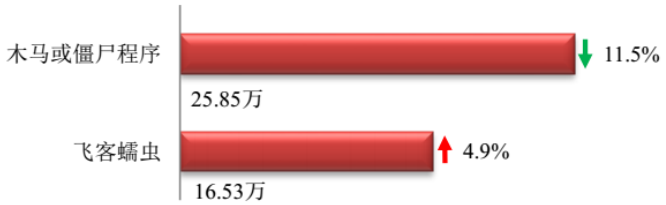
（2017 年 9 月 11 日—9 月 17 日）

根据国家互联网应急中心最新公告数据：



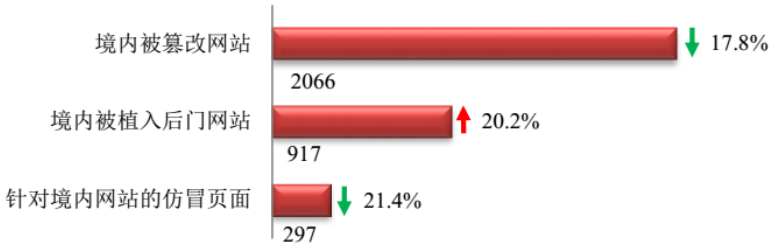
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 42.38 万个，其中包括境内被木马或被僵尸程序控制的主机约 25.85 万以及境内感染飞客（conficker）蠕虫的主机约 16.53 万。



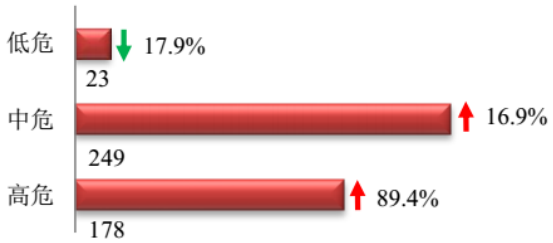
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2066 个；境内被植入后门的网站数量为 917 个；针对境内网站的仿冒页面数量为 297。



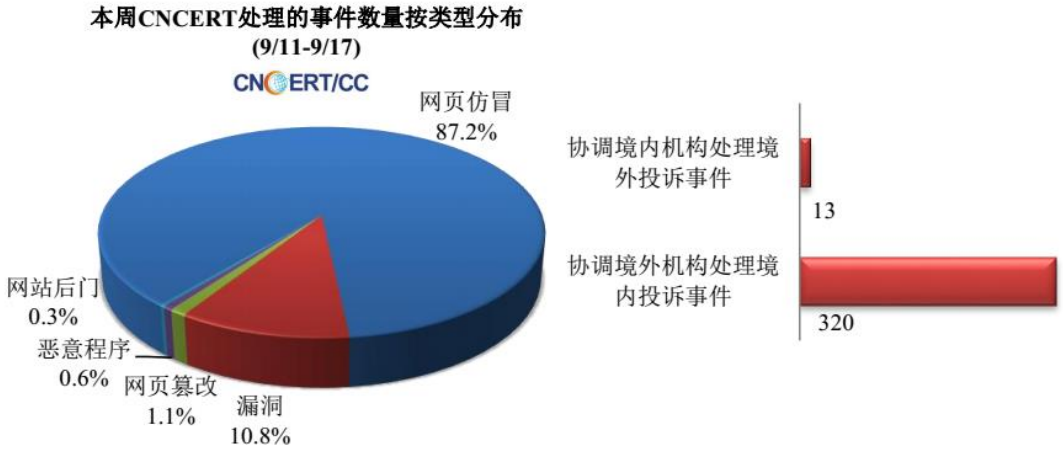
本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 450 个，信息安全漏洞威胁整体评价级别为高。



本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 648 起，其中跨境网络安全事件 333 起。



城院 IT 综合业务管理平台统计信息

（2017 年 9 月 18 日—9 月 24 日）

主要业务服务繁忙度

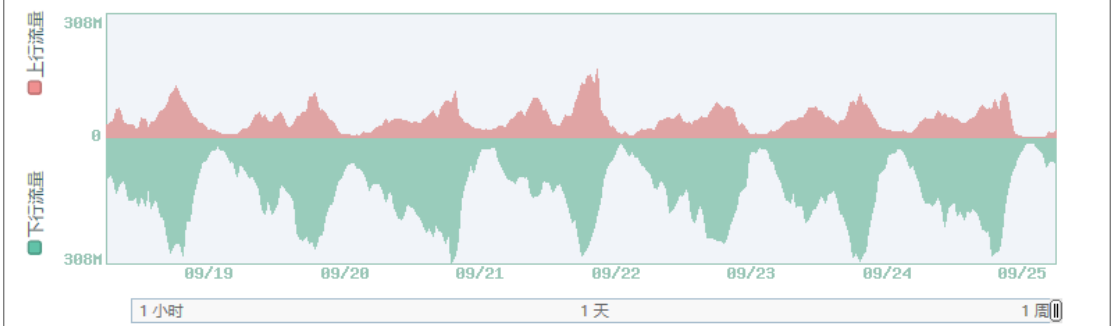
网站集群网页更新情况统计

站点名称	发布		站点名称	发布
兰州城市学院	26		创新创业学院	
马克思主义学院	16		档案馆	
教学质量监测与评估中心	14		党委（校长）办公室	
音乐学院	10		党委宣传部	
党委学生工作部	8		党委组织部	
电子与信息工程学院	6		电子信息科学与技术研究所	
幼儿师范学院	6		发展规划处	
传媒学院	5		甘肃文化翻译中心	
就业服务网	5		甘肃张芝书法院	
商学院	5		国有资产管理处	
数学学院	5		后勤管理处	
外国语学院	5		机关党委	
文史学院	5		基本建设处	
城市社会心理研究中心	4		教师发展中心	
地理与城乡规划学院	4		科学研究处	
廉政网	4		兰州城市学院校医院	
机械工程学院	2		路易艾黎研究中心	
石油工程学院	2		旅游学院	
化学与环境工程学院	1		美术与设计学院	
教务处	1		人事处	
教育学院	1		审计	
卡务中心	1		实训中心	
膳食处	1		体育学院	
信息网络中心	1		团委	
职业技能鉴定所	1		信息技术教育与应用研究所	
保卫处			学位办公室	
城市社会心理研究中心			招生网	
城市信息与系统科学研究所				

网络出口带宽情况统计

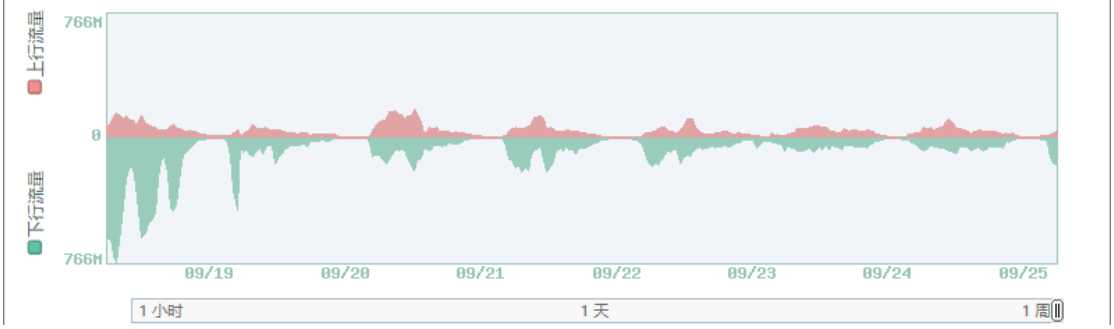
联通出口 - 1 周

接口: Agg_unicom



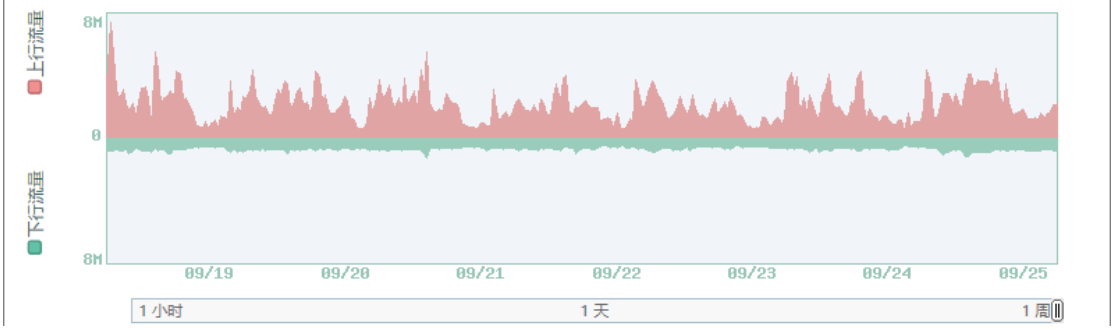
电信出口 - 1 周

接口: Agg_chinanet



教育网出口 - 1 周

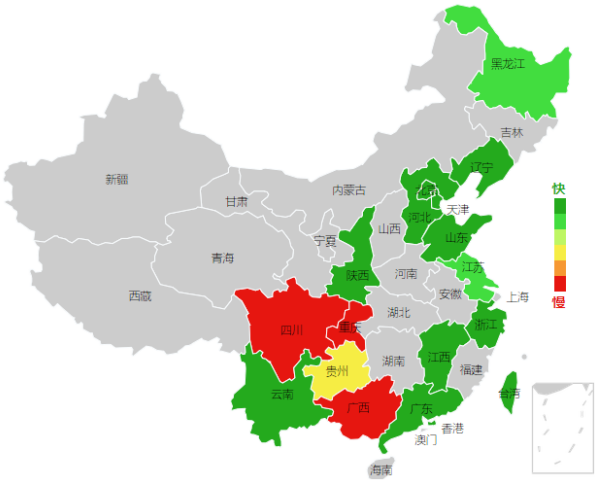
接口: port13



APT统计

防火墙统计	
恶意	2396
检测到0-day恶意软件变种	0
可疑文件	0
清除	75353256

360 网站测速（http://www.lzcu.edu.cn）



平均速度排行		
名次	省份	平均速度(KB/s)
1	陕西	1,147.24
2	山东	454.10
3	天津	447.27

北京					
监测点	运营商	总耗时/ms	解析时间/ms	连接时间/ms	下载时间/ms
北京市	联通	447.94	83.18	49.91	314.86
	电信	1109.05	910.28	30.23	168.54

360 网站评分（http://www.lzcu.edu.cn）

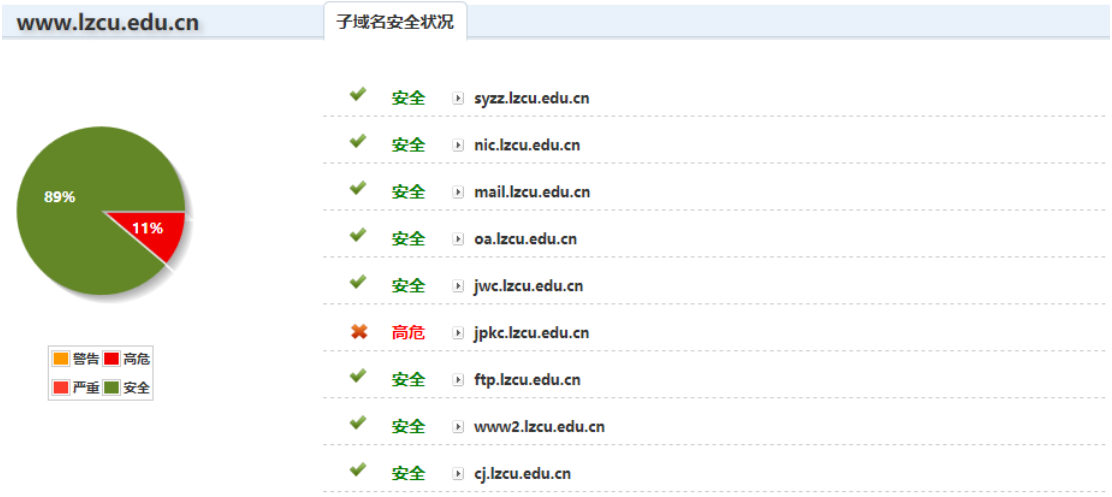
360 网站 DNS 检测（http://www.lzcu.edu.cn）

输入源IP	归属地
219.246.21.192	甘肃兰州教育网

解析结果IP	所用DNS	所属运营商
219.246.21.192	101.226.4.6(上海电信) 123.125.81.6(北京联通) 8.8.8.8(GOOGLE.COMGOOGLE.COMlevel3.com) 121.28.148.33(河北石家庄联通) 114.114.114.114(114DNS.COM114DNS.COM) 168.95.1.1(台湾cht.com.tw) 125.71.5.51(四川成都电信)	电信 联通 其他 联通 其他 其他 电信

网站安全检测一（360 网站安全检测）

注：存在“服务器配置信息泄露”风险，“发现 robots.txt 文件”。



监控对象	类型	监测点	响应时间	访问成功率	
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	4	630.09 ms	100 %	详情
OA办公主页【http://oa.lzcu.edu.cn】	源站监控	4	349.71 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	3	338.14 ms	100 %	详情
WEB【http://www.lzcu.edu.cn】	源站监控	3	1409.44 ms	100 %	详情

网站安全检测二（百度云观测）

http://www.lzcu.edu.cn　　更新时间：2017-09-24 22:16:36

指数评价

34.0

所属行业：教育培训

26.65% ↓

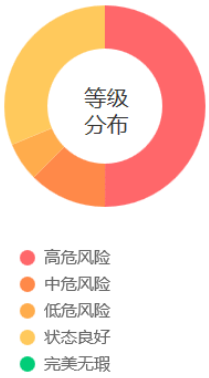
战胜了全国 **0.00%** 的网站

关联网站安全

关联网站数	最低指数评价
16	0 高危

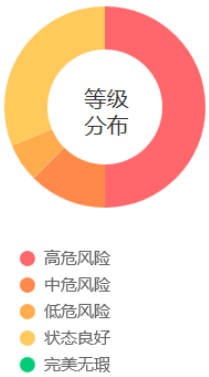
查看更多>>

该网站安全指数评价 高危 但是仍存在改进空间。建议 开启云观测服务>> ，查看评价详情，获取最新网站安全报警，及时修复以免被搜索引擎风险标识或降权。



域名	指数评价	操作
alumni.lzcu.edu.cn	80 良好	查看详情>>
bf.lzcu.edu.cn	4 高危	查看详情>>
cj.lzcu.edu.cn	49 中危	查看详情>>
ecard.lzcu.edu.cn	34 高危	查看详情>>
jpkc2.lzcu.edu.cn	72.2 低危	查看详情>>
jpkc.lzcu.edu.cn	12 高危	查看详情>>
jwc.lzcu.edu.cn	34 高危	查看详情>>
lzcu.edu.cn	80 良好	查看详情>>
nic.lzcu.edu.cn	90 良好	查看详情>>
oa.lzcu.edu.cn	84 良好	查看详情>>

当前 1 / 2 页　首页　上一页　下一页　尾页



域名	指数评价	操作
old.lzcu.edu.cn	44 中危	查看详情>>
pop.lzcu.edu.cn	4 高危	查看详情>>
smtp.lzcu.edu.cn	0 高危	查看详情>>
syzz.lzcu.edu.cn	4 高危	查看详情>>
test.lzcu.edu.cn	84 良好	查看详情>>
www2.lzcu.edu.cn	4 高危	查看详情>>

当前 2 / 2 页　首页　上一页　下一页　尾页

【新闻速递】工信部发布《公共互联网网络安全威胁监测与处置办法》

来源：中国网　时间：2017-09-22

中国网 9 月 15 日消息 记者 9 月 14 日从工信部获悉，工信部制定印发《公共互联网网络安全威胁监测与处置办法》，对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监测处置，并建立网络安全威胁信息共享平台，集成合力维护网络安全。

工信部提出，公共互联网网络安全威胁既包括被用于实施网络攻击的恶意ＩＰ地址、恶意域名、恶意电子信息、恶意程序等，也包括网络服务和产品中存在的安全隐患以及网络安全事件。这些一旦被发现认定，将采取停止服务、屏蔽、清除、通报等措施。

工信部提出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。

工信部网络安全管理局局长赵志国表示，工信部将完善危险监测处置、数据保护、新技术、新业务安全评估等政策，最大限度消除安全隐患，制止攻击行为，避免危害发生。《公共互联网网络安全威胁监测与处置办法》自 2018 年 1 月 1 日起实施。

【安全速递】《公共互联网网络安全威胁监测与处置办法》

发布时间：2017-09-13　来源：网络安全管理局

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。工业和信息化部和各省、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。

抄送：校领导