木马和僵尸网络监测与处置机制

第一条 为有效防范和处置木马和僵尸网络引发的网络安全隐患，规范监测和处置行为，净化网络环境，维护我国公共互联网安全，依据《中华人民共和国电信条例》、《互联网网络安全应急预案》，制定本办法。

第二条 木马是指由攻击者安装在受害者计算机上秘密运行并用于窃取信息及远程控制的程序。僵尸网络是指由攻击者通过控制服务器控制的受害计算机群。木马和僵尸网络对网络信息安全造成危害和威胁，是造成个人隐私泄露、失泄密、垃圾邮件和大规模拒绝服务攻击的重要原因。

第三条 本办法适用于对危害公共互联网安全的木马和僵尸网络控制端（以下简称木马和僵尸网络）及其使用的IP地址和恶意域名的监测和处置。

第四条 工业和信息化部指导、组织、监督全国木马和僵尸网络的监测和处置工作。工业和信息化部通信保障局（以下简称通信保障局）负责具体工作。

各省、自治区、直辖市通信管理局（以下简称通信管理局）指导、组织、监督本行政区域内木马和僵尸网络的监测和处置工作。

国家计算机网络应急技术处理协调中心（以下简称CNCERT）受通信保障局委托，负责对木马和僵尸网络的规模、类型、活跃程度、危害等情况进行监测、汇总、分析、核实，组织开展通报工作，协调处置木马和僵尸网络IP地址和恶意域名。

基础电信运营企业负责对本单位网内木马和僵尸网络进行监测、核实，对CNCERT汇总通报的涉及本单位的木马和僵尸网络进行处置和反馈。

互联网域名注册管理机构负责对CNCERT通报的由自身管理的恶意域名进行处置。对于由国内互联网域名注册服务机构注册的由境外域名注册管理机构管理的域名，由CNCERT直接协调国内互联网域名注册服务机构进行处置。

第五条 基础电信运营企业、互联网接入服务提供商、IDC服务提供商、互联网域名注册管理机构、国内互联网域名注册服务机构在提供互联网接入服务、域名解析服务时，应在与用户签订的服务协议、合同中告知用户承担的网络安全保障责任。

第六条 CNCERT、基础电信运营企业应不断提高木马和僵尸网络的监测能力。CNCERT、基础电信运营企业、互联网域名注册管理机构、国内互联网域名注册服务机构应建立健全本单位的处置机制，协同配合、快速处置，共同做好木马和僵尸网络的监测和处置工作。

第七条 木马和僵尸网络事件分为特别重大、重大、较大、一般共四级。

特别重大事件：涉及全国范围或省级行政区域，单个木马和僵尸网络规模超过100万个IP地址，对社会造成特别重大影响。

重大事件：涉及全国范围或省级行政区域，同一时期存在一个或多个木马和僵尸网络，总规模超过50万个IP地址，对社会造成重大影响。

较大事件：涉及全国范围或省级行政区域，同一时期存在一个或多个木马和僵尸网络，总规模超过10万个IP地址，对社会造成较大影响。

一般事件：涉及全国范围或省级行政区域，发生木马和僵尸网络事件，对社会造成一定影响，但未造成上述后果。

通信保障局负责对分级规范进行修订。

第八条 监测和通报：

（一）CNCERT、基础电信运营企业负责对木马和僵尸网络进行监测。

（二）基础电信运营企业按照本机制第七条对监测到的事件进行分级，特别重大、重大、较大事件应在发现后2小时内报送通信保障局，同时抄报CNCERT；一般事件应在发现后5个工作日内报送CNCERT。

报送内容包括：控制端IP地址、端口、发现时间及其使用的恶意域名。

（三）CNCERT汇总自主监测、基础电信运营企业报送和从其他渠道收集的事件，进行综合分析、分级。对于特别重大、重大、较大事件，CNCERT应在2小时内向通信保障局报告，并及时通报相关通信管理局。通信保障局认为必要时，组织有关单位和专家进行研判。事件情况及研判结果由通信保障局直接或委托CNCERT通报相关单位。对于一般事件，CNCERT应在发现后5个工作日内通报相关单位。

事件通报内容包括：

1、威胁较大的木马和僵尸网络IP地址、端口、发现时间、所属基础电信运营企业。

2、木马和僵尸网络使用的恶意域名。

3、木马和僵尸网络的规模和潜在危害。

监测和通报流程图见附件一。

第九条 处置和反馈：

基础电信运营企业、互联网域名注册管理机构、互联网域名注册服务机构接到CNCERT木马和僵尸网络事件通报后，应按如下流程处理：

（一）通知与木马和僵尸网络IP地址和恶意域名相关的具体用户进行清除，并跟踪用户处置情况。

对于域名注册信息不真实、不准确、不完整的，互联网域名注册管理机构、互联网域名注册服务机构根据《中国互联网域名管理办法》有关规定进行处置。

（二）反馈用户的处置情况。特别重大、重大、较大事件的处置情况应在接到事件通报后4小时内向CNCERT反馈，一般事件的处置情况应在5个工作日内向CNCERT反馈。

反馈内容包括：用户已处置的IP地址和恶意域名、单位名称、用户未处置的IP地址和恶意域名及未处置的原因。

（三）监测单位验证处置情况。

对于CNCERT自主监测的事件，由CNCERT对处置情况进行验证。特别重大、重大、较大事件应在接到处置单位反馈后2小时内向处置单位反馈验证结果，一般事件应在5个工作日内反馈验证结果。

对于基础电信运营企业监测到的事件由基础电信运营企业自行验证。特别重大、重大、较大事件应在接到CNCERT事件通报后6小时内向CNCERT反馈验证结果，一般事件应在10个工作日内向CNCERT反馈验证结果。

（四）对于未处置或经验证仍存在恶意连接的木马和僵尸网络IP地址和恶意域名，按如下方式处置：

对于重要信息系统单位，向通信保障局反馈用户相关情况，抄报CNCERT，由通信保障局或当地通信管理局书面通知其主管部门。

对于其他单位用户和个人用户，应依据与用户签署的服务协议、合同等进行处置。

（五）对于特别重大、重大、较大事件的处置情况，CNCERT应在接到处置单位反馈后2小时内向通信保障局和相关通信管理局反馈处置结果，一般事件处置情况由CNCERT每月汇总，按照互联网网络安全信息通报有关办法通报监测和处置情况。

处置和反馈流程见附件二。

第十条 CNCERT、基础电信运营企业、互联网域名注册管理机构、国内互联网域名注册服务机构应留存木马和僵尸网络相关数据或资料以备查验。数据或资料保存时间为60天。

第十一条 CNCERT、基础电信运营企业、互联网域名注册管理机构、国内域名注册服务机构应保护用户正当权益，规范处置流程，建立用户申诉机制，妥善解决用户争议。

第十二条 通信保障局通过会商制度，组织相关单位和专家研讨木马和僵尸网络相关问题及其应对策略。

第十三条 事件通报和反馈应按照统一表格以书面方式报送（报送格式见附件三）。紧急情况下，可以先电话联系，后补表格。

第十四条 对于国家举办重要活动等特殊时期，对木马和僵尸网络监测和处置工作另有要求的，从其规定。

第十五条 相关单位应将本单位木马和僵尸网络监测和处置工作主管领导，责任部门负责人、联系人、联系方式报送通信保障局，抄送CNCERT。以上信息发生变更，应在3个工作日内报送变更情况。

第十六条 CNCERT应与非经营性互联单位合作，协调非经营性互联单位处置其网内木马和僵尸网络；应与网络安全研究机构、网络安全技术支撑单位、网络安全企业、病毒厂商等单位合作，建立研究、分析机制。

本机制中非经营性互联单位指中国教育和科研计算机网、中国科技网、中国国际经济贸易网、中国长城互联网。

第十七条 对于涉嫌犯罪的木马和僵尸网络事件，应报请公安机关依法调查处理。

第十八条 通信管理局应参照本办法制定本行政区域内木马和僵尸网络监测和处置机制。

基础电信运营企业集团公司应督促本单位省级公司按照当地通信管理局要求，及时反馈木马和僵尸网络事件监测处置情况，接受当地通信管理局的监督管理。

第十九条 本办法中重要信息系统指政府部门、军队以及银行、海关、税务、电力、铁路、证券、保险、民航等关系国计民生的重要行业使用的信息系统。

第二十条 本办法自2009年6月1日起实施。
附件一：监测和通报流程图（ [下载](http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4062282/n4062316/n4062350/n4062351/c4098193/part/4098194.pdf%22%20%5Ct%20%22_blank)）
附件二：处置和反馈流程图（ [下载](http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4062282/n4062316/n4062350/n4062351/c4098193/part/4098195.pdf)）
附件三：事件通报表格（ [下载](http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4062282/n4062316/n4062350/n4062351/c4098193/part/4098196.doc)）
附件四：联系方式
（1）通信保障局
主管领导： 熊四皓 010-66069910
联 系 人： 闫宏强 010-66069895，13011881107
付景广 010-66022774，13701353949

（2）工业和信息化部24小时值班电话：010-66014249

（3）CNCERT
主管领导：云晓春 010－82990501
联 系 人：孙蔚敏 010－82990103 13911218086
          温森浩 010－82990680 13810059765
CNCERT 24小时值班电话：010－82990999