**移动互联网恶意程序监测与处置机制**

第一条 为净化公共互联网网络环境，保护用户权益，维护网络安全，有效防范和处置移动互联网恶意程序，依据《中华人民共和国电信条例》、《公共互联网网络安全应急预案》，制定本机制。

第二条 移动互联网恶意程序是指运行于包括智能手机在内的具有移动通信功能的移动终端之上，存在窃听用户通话、窃取用户信息、破坏用户数据、擅自使用付费业务、发送垃圾信息、推送广告或欺诈信息、影响移动终端运行、危害互联网网络安全等恶意行为的计算机程序。

第三条 本机制适用于移动互联网恶意程序及其传播服务器、控制服务器的监测和处置。

第四条 工业和信息化部指导、组织、监督全国移动互联网恶意程序的监测和处置工作。工业和信息化部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、监督本行政区域内移动互联网恶意程序的监测和处置工作。

国家计算机网络应急技术处理协调中心（以下简称CNCERT）受工业和信息化部委托，负责对移动互联网恶意程序样本进行认定命名，对移动互联网恶意程序进行监测、分析、通报，协调处置传播服务器、控制服务器和攻击源。

移动通信运营企业负责报送移动互联网恶意程序疑似样本，对CNCERT认定通报的移动互联网恶意程序进行监测、处置和反馈，为本单位所服务的用户提供信息提示和查杀技术咨询。

互联网域名注册管理机构和注册服务机构负责对CNCERT通报的由自身管理的恶意域名进行处置。

第五条 移动通信运营企业、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、互联网域名注册服务机构在提供互联网接入服务、托管服务、域名注册解析等服务时，应在与用户签订的服务协议、合同中约定用户承担的网络安全保障责任。

第六条 移动通信运营企业、CNCERT应不断提高移动互联网恶意程序的样本捕获和监测处置能力，建设完善相关技术平台。移动通信运营企业应具备覆盖本企业网内的监测处置能力,CNCERT应具备跨不同企业移动互联网的监测能力。

第七条 CNCERT、移动通信运营企业、互联网域名注册管理和服务机构应建立健全本单位的处置机制，加强协同配合，共同做好移动互联网恶意程序的监测和处置工作。

第八条 移动互联网恶意程序事件分为特别重大、重大、较大、一般共四级。

特别重大事件：单个移动互联网恶意程序造成用户通信费用损失累计超过一千万元人民币，或24小时内受感染用户规模超过十万个手机号码，对社会造成特别重大影响。

重大事件：单个移动互联网恶意程序造成用户通信费用损失累计超过五百万元人民币，或24小时内受感染用户规模超过五万个手机号码，对社会造成重大影响。

较大事件：单个移动互联网恶意程序造成用户通信费用损失累计超过一百万元人民币，或24小时内受感染用户规模超过一万个手机号码，对社会造成较大影响。

一般事件：发生移动互联网恶意程序事件，对社会造成一定影响，但未造成上述后果。

工业和信息化部负责对分级规范进行修订。

第九条 样本捕获与认定命名

（一）移动通信运营企业自主捕获或从其他渠道获得疑似恶意程序样本，应于发现后进行初步分析并提出命名建议，在3个工作日内将样本和分析结果报送CNCERT（报送格式见附件一）。

（二）CNCERT汇总自主捕获、移动通信运营企业报送和从其他渠道收集的疑似恶意程序样本，依据《移动互联网恶意程序描述格式》进行分析、认定和命名，将认定结果和处置建议在5个工作日内反馈各样本报送单位和相关通信管理局（反馈格式见附件二）。

第十条 事件监测和通报

（一）CNCERT、移动通信运营企业负责对移动互联网恶意程序进行监测。

（二）移动通信运营企业按照本机制第八条规定，对监测到的事件进行分级。特别重大、重大事件应在发现后2小时内报工业和信息化部，同时抄报相关通信管理局和CNCERT；较大事件应在发现后4小时内报送工业和信息化部，同时抄报相关通信管理局和CNCERT；一般事件应按约定电子接口方式报CNCERT汇总（较大以上事件报送格式见附件三）。

（三）CNCERT汇总自主监测、移动通信运营企业报送和从其他渠道收集的移动互联网恶意程序事件，对事件情况开展综合分析、分级。特别重大、重大事件应在发现后2小时内报工业和信息化部，同时抄报相关通信管理局；较大事件应在发现后4小时内报送工业和信息化部，同时抄报相关通信管理局。工业和信息化部认为必要时，组织有关单位和专家进行研判。事件情况及研判结果由工业和信息化部直接或委托CNCERT通报相关单位。一般事件由CNCERT每月汇总，按照互联网网络安全信息通报办法规定通报监测情况（较大以上事件通报格式见附件四）。

第十一条 事件处置和反馈

CNCERT、移动通信运营企业、互联网域名注册管理和服务机构应按如下要求进行处置：

（一）移动通信运营企业通过自有的移动互联网恶意程序监测处置平台采取处置措施。对于特别重大、重大和较大事件，向本单位所服务的用户提供信息提示和查杀技术咨询。

（二）互联网域名注册管理机构和注册服务机构对移动互联网恶意程序控制服务器和传播服务器使用的恶意域名进行处置。

（三）CNCERT对境外注册的恶意域名进行协调处置。

（四）反馈事件的处置情况。特别重大、重大事件的处置情况应在接到事件通报后2小时内向CNCERT反馈；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按月度汇总后以电子表格形式向CNCERT反馈（较大以上事件反馈格式见附件五）。

（五）CNCERT验证处置情况。特别重大、重大事件应在接到处置单位反馈后2小时内向工业和信息化部、相关通信管理局和处置单位反馈验证结果；较大事件应在接到处置单位反馈后4小时内向工业和信息化部、相关通信管理局和处置单位反馈验证结果；一般事件无需验证。

第十二条 CNCERT、移动通信运营企业、互联网域名注册管理机构和注册服务机构应留存所监测和处置的移动互联网恶意程序相关数据或资料以备查验。数据或资料保存时间为60天。

第十三条 CNCERT、移动通信运营企业、互联网域名注册管理机构和注册服务机构应保护用户正当权益，加强用户信息保护，规范处置流程，建立用户投诉机制，妥善解决用户争议。

第十四条 工业和信息化部建立会商制度，组织相关单位和专家研讨移动互联网恶意程序相关问题及应对策略。

第十五条 较大以上事件通报和反馈应按照统一表格以书面方式报送，紧急情况下，可以先通过电话、电子邮件等方式联系，后补书面材料。

第十六条 对于国家举办重要活动等特殊时期，对移动互联网恶意程序监测和处置工作另有要求的，从其规定。

第十七条 相关单位应将本单位移动互联网恶意程序监测和处置工作主管领导和责任部门负责人、联系人、联系方式报送工业和信息化部，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。

第十八条 对于涉嫌制作、传播恶意程序或利用恶意程序牟利的移动互联网服务提供商及其他合作伙伴等，移动通信运营企业应依据双方签订的合同，对其进行处理，并报当地通信管理局依法处罚。对于涉嫌犯罪的事件，应报请公安机关依法调查处理。

第十九条 各单位开展信息报送应遵循及时、客观、准确、完整的原则，不得迟报、谎报、瞒报和漏报。工业和信息化部定期对各单位信息报送情况进行通报。

第二十条 各通信管理局应依据本机制落实本行政区域内相关工作。

第二十一条 本机制自2012年1月1日起执行。

附件一：移动互联网疑似恶意程序样本报送表

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **移动互联网疑似恶意程序样本报送表** | | | | | | | | | | |
| 填报单位： | | | | | | 填报人： | | 填报时间：       年   月   日 | | |
| 序号 | 首次获取 样本时间 | 恶意程序建议名称 | 恶意程序建议 中文名称 | 建议危害等级 | 典型行为 | MD5值 | 控制域名或IP | 恶意程序请求URL | 样本 来源 | 备注 |
| 1 |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |

附件二：移动互联网恶意程序样本认定信息表

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **移动互联网恶意程序样本认定信息表** | | | | | | | | | | | |
| 编号： | | | | | | 认定人： | | 认定时间：       年   月   日 | | | |
| 序号 | 首次获取 样本时间 | 恶意程序规范名称 | 恶意程序中文名称 | 危害 等级 | 典型行为 | MD5值 | 控制域名 | 恶意程序请求URL | 样本 来源 | 处置建议 | 备注 |
| 1 |  |  |  |  |  |  |  |  |  |  |  |
| 2 |  |  |  |  |  |  |  |  |  |  |  |
| 3 |  |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |  |
| 6 |  |  |  |  |  |  |  |  |  |  |  |
| 7 |  |  |  |  |  |  |  |  |  |  |  |
| 8 |  |  |  |  |  |  |  |  |  |  |  |
| 9 |  |  |  |  |  |  |  |  |  |  |  |
| 10 |  |  |  |  |  |  |  |  |  |  |  |
| 11 |  |  |  |  |  |  |  |  |  |  |  |
| 12 |  |  |  |  |  |  |  |  |  |  |  |

附件三：较大以上移动互联网恶意程序事件报送表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **较大以上移动互联网恶意程序事件报送表**  **（报送单位：                 ）** | | | | | |
| **报：**  **抄报：** | | | | | |
| 填报人 |  | 联系电话 |  | E-Mail |  |
| 发生时间 |  | | 报送时间 |  | |
| 恶意程序名称 |  | | | | |
| 事件简要描述 |  | | | | |
| 控制服务器IP地址及其使用的域名、端口 |  | | | | |
| 传播服务器IP地址及其使用的域名、端口 |  | | | | |
| 受感染移动智能终端数量 |  | | | | |
| 主要行为特征 |  | | | | |
| 潜在危害 |  | | | | |
| 备注 |  | | | | |

附件四：较大以上移动互联网恶意程序事件信息通报

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **较大以上移动互联网恶意程序事件信息通报** | | | | | |
| **报：**  **抄报：** | | | | | |
| 任务编号： | | | | | |
| 填报人 |  | 联系电话 |  | E-Mail |  |
| 发生时间 |  | | 报送时间 |  | |
| 恶意程序名称 |  | | | | |
| 所属移动通信运营企业 |  | | 影响的移动智能终端系统类型、版本 |  | |
| 事件简要描述 |  | | | | |
| 控制服务器IP地址及其使用的域名、端口 |  | | | | |
| 传播服务器IP地址及其使用的域名、端口 |  | | | | |
| 受感染移动智能终端数量 |  | | | | |
| 主要行为特征 |  | | | | |
| 潜在危害 |  | | | | |
| 备注 |  | | | | |

附件五：较大以上移动互联网恶意程序处置反馈表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **较大以上移动互联网恶意程序处置反馈表**  **（报送单位：                 ）** | | | | | |
| **报：**  **抄报：** | | | | | |
| 任务编号： | | | | | |
| 填报人 |  | 联系电话 |  | E-Mail |  |
| 处置时间 |  | | 反馈时间 |  | |
| 恶意程序名称 |  | | | | |
| 已处置的控制服务器IP地址及其使用的域名、端口 |  | | | | |
| 已处置的传播服务器IP地址及其使用的域名、端口 |  | | | | |
| 已直接提示的用户数量 |  | | | | |
| 未处置的控制服务器IP地址及其使用的域名、端口 |  | | | | |
| 未处置的传播服务器IP地址及其使用的域名、端口 |  | | | | |
| 未处置的原因 |  | | | | |
| 备注 |  | | | | |
| 验证结果  *由CNCERT填写* |  | | | | |