移动互联网恶意程序描述格式

1 范围

本标准规定了移动互联网恶意程序的定义、行为属性、判定及命名格式。

本标准适用于移动互联网恶意程序认定及恶意程序信息数据交换。

2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

3 术语和定义

下列术语和定义适用于本标准。

3.1 移动互联网恶意程序

在用户不知情或未授权的情况下，在移动终端系统中安装、运行以达到不正当目的，或具有违反国家相关法律法规行为的可执行文件、程序模块或程序片段。

3.2 移动互联网恶意程序样本

存放移动互联网恶意程序的文件实体，可以是独立的恶意程序载体文件、被感染型恶意程序感染后的文件，也可以是非文件载体恶意程序的文件镜像（包括但不限于引导型恶意程序的文件镜像、内存恶意程序的文件镜像）。

3.3 移动互联网恶意程序主体

能够完成恶意程序行为的全部可执行文件及其必要的关联文件(包括但不限于库文件、配置文件等）的集合。

3.4 移动互联网恶意程序安装包

包含移动互联网恶意程序主体的安装载体，可以在相应版本的移动终端系统中安装运行。

4 移动互联网恶意程序行为属性及判定

4.1 用户不知情或未授权情况

本文所述“用户不知情或未授权的情况”包括但不限于以下情况：

——未向用户明确提示所要执行的全部功能及可能产生的资费，并请用户做出选择的；

——用户选择“否”、“不同意”、“取消”、“不允许”、“卸载”等选项的；

——用户选择“是”、“同意”、“确认”、“允许”、“安装”等选项，但并未对其隐藏的行为明确知情或授权的；

——通过捆绑、诱骗等手段致使用户点击“是”、“同意”、“确认”、“允许”、“安装”等按钮的。

4.2 移动互联网恶意程序行为属性分类

4.2.1 恶意扣费

在用户不知情或未授权的情况下，通过隐蔽执行、欺骗用户点击等手段，订购各类收费业务或使用移动终端支付，导致用户经济损失的，具有恶意扣费属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有恶意扣费属性：

——在用户不知情或未授权的情况下，自动订购移动增值业务的；

——在用户不知情或未授权的情况下，自动利用移动终端支付功能进行消费的；

——在用户不知情或未授权的情况下，自动拨打收费声讯电话的；

——在用户不知情或未授权的情况下，自动订购其它收费业务的；

——在用户不知情或未授权的情况下，自动通过其它方式扣除用户资费的。

4.2.2 信息窃取

在用户不知情或未授权的情况下，获取涉及用户个人信息、工作信息或其它非公开信息的，具有信息窃取属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有信息窃取属性：

——在用户不知情或未授权的情况下，获取短信内容的；

——在用户不知情或未授权的情况下，获取彩信内容的；

——在用户不知情或未授权的情况下，获取邮件内容的；

——在用户不知情或未授权的情况下，获取通讯录内容的；

——在用户不知情或未授权的情况下，获取通话记录的；

——在用户不知情或未授权的情况下，获取通话内容的；

——在用户不知情或未授权的情况下，获取地理位置信息的；

——在用户不知情或未授权的情况下，获取本机手机号码的；

——在用户不知情或未授权的情况下，获取本机已安装软件信息的；

——在用户不知情或未授权的情况下，获取本机运行进程信息的；

——在用户不知情或未授权的情况下，获取用户各类帐号信息的；

——在用户不知情或未授权的情况下，获取用户各类密码信息的；

——在用户不知情或未授权的情况下，获取用户文件内容的；

——在用户不知情或未授权的情况下，记录分析用户行为的；

——在用户不知情或未授权的情况下，获取用户网络交易信息的；

——在用户不知情或未授权的情况下，获取用户收藏夹信息的；

——在用户不知情或未授权的情况下，获取用户联网信息的；

——在用户不知情或未授权的情况下，获取用户下载信息的；

——在用户不知情或未授权的情况下，利用移动终端麦克风、摄像头等设备获取音频、视频、图片信息的；

——在用户不知情或未授权的情况下，获取用户其它个人信息的；

——在用户不知情或未授权的情况下，获取用户其它工作信息的；

——在用户不知情或未授权的情况下，获取其它非公开信息的。

4.2.3 远程控制

在用户不知情或未授权的情况下，能够接受远程控制端指令并进行相关操作的，具有远程控制属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有远程控制属性：

——由控制端主动发出指令进行远程控制的；

——由受控端主动向控制端请求指令的。

4.2.4 恶意传播

自动通过复制、感染、投递、下载等方式将自身、自身的衍生物或其它恶意程序进行扩散的行为，具有恶意传播属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有恶意传播属性：

——自动发送包含恶意程序链接的短信、彩信、邮件、WAP信息等；

——自动发送包含恶意程序的彩信、邮件等；

——自动利用蓝牙通讯技术向其它设备发送恶意程序的；

——自动利用红外通讯技术向其它设备发送恶意程序的；

——自动利用无线网络技术向其它设备发送恶意程序的；

——自动向存储卡等移动存储设备上复制恶意程序的；

——自动下载恶意程序的；

——自动感染其它文件的。

4.2.5 资费消耗

在用户不知情或未授权的情况下，通过自动拨打电话、发送短信、彩信、邮件、频繁连接网络等方式，导致用户资费损失的，具有资费消耗属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有资费消耗属性：

——在用户不知情或未授权的情况下，自动拨打电话的；

——在用户不知情或未授权的情况下，自动发送短信的；

——在用户不知情或未授权的情况下，自动发送彩信的；

——在用户不知情或未授权的情况下，自动发送邮件的；

——在用户不知情或未授权的情况下，频繁连接网络，产生异常数据流量的。

4.2.6 系统破坏

通过感染、劫持、篡改、删除、终止进程等手段导致移动终端或其它非恶意软件部分或全部功能、用户文件等无法正常使用的，干扰、破坏、阻断移动通信网络、网络服务或其它合法业务正常运行的，具有系统破坏属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有系统破坏属性：

——导致移动终端硬件无法正常工作的；

——导致移动终端操作系统无法正常运行的；

——导致移动终端其它非恶意软件无法正常运行的；

——导致移动终端网络通讯功能无法正常使用的；

——导致移动终端电池电量非正常消耗的；

——导致移动终端发射功率异常的；

——导致运营商通信网络无法正常工作的；

——导致其它合法业务无法正常运行的；

——对用户文件、系统文件或其它非恶意软件进行感染、劫持、篡改的；

——在用户不知情或未授权的情况下，对系统文件或其它非恶意软件进行删除、卸载、终止进程或限制运行的；

——在用户不知情或未授权的情况下，对用户文件进行删除的。

4.2.7 诱骗欺诈

通过伪造、篡改、劫持短信、彩信、邮件、通讯录、通话记录、收藏夹、桌面等方式，诱骗用户，而达到不正当目的的，具有诱骗欺诈属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有诱骗欺诈属性：

——伪造、篡改、劫持短信，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持彩信，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持邮件，以诱骗用户，而达到不正当目的的；

——伪造、篡改通讯录，以诱骗用户，而达到不正当目的的；

——伪造、篡改收藏夹，以诱骗用户，而达到不正当目的的；

——伪造、篡改通讯记录，以诱骗用户，而达到不正当目的的；

——伪造、篡改、劫持用户文件，以诱骗用户，而达到不正当目的的。

——伪造、篡改、劫持用户网络交易数据，以诱骗用户，而达到不正当目的的；

——冒充国家机关、金融机构、移动终端厂商、运营商或其它机构和个人，以诱骗用户，而达到不正当目的的；

——伪造事实，诱骗用户退出、关闭、卸载、禁用或限制使用其它合法产品或退订服务的。

4.2.8 流氓行为

执行对系统没有直接损害，也不对用户个人信息、资费造成侵害的其它恶意行为具有流氓行为属性。

包括但不限于具有以下任意一种行为的移动互联网恶意程序具有流氓行为属性：

——在用户不知情或未授权的情况下，长期驻留系统内存的；

——在用户不知情或未授权的情况下，长期占用移动终端中央处理器计算资源的；

——在用户不知情或未授权的情况下，自动捆绑安装的；

——在用户不知情或未授权的情况下，自动添加、修改、删除收藏夹、快捷方式的；

——在用户未授权的情况下，弹出广告窗口的；

——导致用户无法正常退出程序的；

——导致用户无法正常卸载、删除程序的；

——在用户未授权的情况下，执行其它操作的。

4.3 移动互联网恶意程序判定

当一个可运行于移动终端上的程序具有 4.2 节所述一种或多种行为属性时，可判定为移动互联网恶意程序。

5 移动互联网恶意程序命名格式

5.1 移动互联网恶意程序命名格式

移动互联网恶意程序采用分段式格式命名，前四段为必选项，使用英文（不区分大小写）或数字标识；第五段起为扩展字段，扩展字段为可选项，内容使用中括号“[]”标识，可使用任何Unicode字符，扩展字段可增加多个。命名格式如下：

受影响操作系统编码.恶意程序属性主分类编码.恶意程序名称.变种名称.[扩展字段]

如：

——s.remote.dumusicplay.b.[毒媒]

——a.remote.adrd.a.[红透透]

——s.remote.dumusicplay.f.[毒媒].[已升级]

——w.privacy.mobilespy.c

——i.spread.ikee.a

——b.privacy.txsbbspy.a

——p.remote.vapor.a

——j.payment.swapi.e

5.2 受影响操作系统编码

受影响操作系统及编码包括但不限于以下类型：

——a：Android

——b：Black Berry

——bd：Bada

——i：IPhone IOS

——j：J2ME(Java 2 Micro Edition)

——m：MTK

——p：Palm OS

——s：Symbian

——w：Windows Mobile\WinCE\Windows Phone

——o：其它类型的平台

5.3 恶意程序属性主分类编码

本标准将移动互联网恶意程序属性按危害程度及包含关系排序，如某恶意程序具有多个属性，则以排序靠前的属性作为主分类，以便于对其进行描述，方便公众识别。

移动互联网恶意程序属性主分类编码及排序如表 1 所示：

表 1 主分类编码

排序	编码	属性主分类
1	payment	恶意扣费
2	privacy	信息窃取
3	remote	远程控制
4	spread	恶意传播
5	expense	资费消耗
6	system	系统破坏
7	fraud	诱骗欺诈
8	rogue	流氓行为

5.4 恶意程序名称

移动互联网恶意程序主体功能不相同的，可命名为不同名称。移动互联网恶意程序名称可使用解开

安装包或压缩格式后的恶意程序主程序的可执行文件名、主要进程的名称或特征字符串命名，亦可使用主程序体中第一个可用的ASCII码串命名。原则上应遵循使用第一个公开报告的名称。

恶意程序的中文名称可参见 5.6 节，置于扩展字段内。

5.5 变种名称

移动互联网恶意程序主体功能相同，但配置不同的，则认为是同一家族的恶意程序，这时需要用变种名称来区分。变种名称根据样本发现顺序采用英文字母依次命名。第一个发现的样本命名为a，第二个命名为b，第 27 个发现的样本命名为aa，第 28 个命名为ab，以此类推。

移动互联网恶意程序主体功能相同，配置也相同，但HASH值不完全相同，则认为是不同HASH值的同一恶意程序的同一变种，其名称及变种名称均应完全相同。

5.6 扩展字段

扩展字段主要用于补充标识前四段必选项无法标示的其它重要信息，如中文通用名称等。

扩展字段中的通用中文名称可使用安装包的中文名称、可执行文件运行界面的中文名称、进程连接的网站名称等。原则上应遵循使用第一个公开报告的名称。