



CNCERT互联网安全威胁报告

2018年4月 总第88期



摘要:

本报告以 CNCERT 监测数据和通报成员单位报送数据作为主要依据,对我国互联网面临的各类安全威胁进行总体态势分析,并对重要预警信息和典型安全事件进行探讨。

2018年4月,互联网网络安全状况整体评价为良。主要数据如下:

- 境内感染网络病毒的终端数为近85万余个;
- 境内被篡改网站数量为1,866个,其中被篡改政府网站数量为52个;境内被植入后门的网站数量为3,280个,其中政府网站有82个;针对境内网站的仿冒页面数量为3,440个;
- 国家信息安全漏洞共享平台(CNVD)收集整理信息系统安全漏洞1,130个,其中,高危漏洞374个,可被用来实施远程攻击的漏洞有992个。

热线电话: +8610 82990999 (中文), 82991000 (英文) 传真: +8610 82990399

电子邮件: cncert@cert.org.cn

PGP Key: <http://www.cert.org.cn/cncert.asc>

网址: <http://www.cert.org.cn/>

关于国家互联网应急中心 (CNCERT)

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称(英文简称为CNCERT或CNCERT/CC),成立于2002年9月,为非政府非盈利的网络安全技术中心,是我国网络安全应急体系的核心协调机构。

2003年,CNCERT在全国31个省(直辖市、自治区)成立分中心。作为国家级应急中心,CNCERT的主要职责是:按照“积极预防、及时发现、快速响应、力保恢复”的方针,开展互联网网络安全事件的预防、发现、预警和协调处置等工作,维护国家公共互联网安全,保障基础信息网络和重要信息系统的安全运行。

CNCERT的业务能力如下:

事件发现——依托“公共互联网网络安全监测平台”,开展对基础信息网络、金融证券等重要信息系统、移动互联网服务提供商、增值电信企业等安全事件的自主监测。同时还通过与国内外合作伙伴进行数据和信息共享,以及通过热线电话、传真、电子邮件、网站等接收国内外用户的网络安全事件报告等多种渠道发现网络攻击威胁和网络安全事件。

预警通报——依托对丰富数据资源的综合分析和多渠道的信息获取,实现网络安全威胁的分析预警、网络安全事件的情况通报、宏观网络安全状况的态势分析等,为用户单位提供互联网网络安全态势信息通报、网络安全技术和资源信息共享等服务。

应急处置——对于自主发现和接收到的危害较大的事件报告,CNCERT及时响应并积极协调处置,重点处置的事件包括:影响互联网运行安全的事件、波及较大范围互联网用户的事件、涉及重要政府部门和重要信息系统的事件、用户投诉造成较大影响的事件,以及境外国家级应急组织投诉的各类网络安全事件等。

测试评估——作为网络安全检测、评估的专业机构,按照“支撑监管,服务社会”的原则,以科学的方法、规范的程序、公正的态度、独立的判断,按照相关标准为政府部门、企事业单位提供安全评测服务。CNCERT还组织通信网络安全相关标准制定,参与电信网和互联网安全防护系列标准的编制等。

同时,作为中国非政府层面开展网络安全事件跨境处置协助的重要窗口,CNCERT积极开展国际合作,致力于构建跨境网络安全事件的快速响应和协调处置机制。CNCERT为国际著名网络安全合作组织FIRST正式成员以及亚太应急组织APCERT的发起人之一。截止2017年,CNCERT与72个国家和地区的211个组织建立了“CNCERT国际合作伙伴”关系。

版权及免责声明

《CNCERT 互联网安全威胁报告》(以下简称“报告”)为国家计算机网络应急技术处理协调中心(简称国家互联网应急中心, CNCERT 或 CNCERT/CC)的电子刊物, 由 CNCERT 编制并拥有版权。报告中凡摘录或引用内容均已指明出处, 其版权归相应单位所有。本报告所有权利及许可由 CNCERT 进行管理, 未经 CNCERT 同意, 任何单位或个人不得将本报告以及其中内容转发或用于其他用途。

CNCERT 力争保证本报告的准确性和可靠性, 其中的信息、数据、图片等仅供参考, 不作为您个人或您企业实施安全决策的依据, CNCERT 不承担与此相关的一切法律责任。

编者按：

感谢您阅读《CNCERT 互联网安全威胁报告》，如果您发现本报告存在任何问题，请您及时与我们联系，来信地址为：cn-cert@cert.org.cn。

本月网络安全基本态势分析

2018年4月，互联网网络安全状况整体评价为良。我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未发生较大以上网络安全事件。在我国公共互联网网络安全环境方面，除木马或僵尸程序控制服务器IP地址数量、境内感染木马或僵尸程序的IP地址数量和境内被植入后门的网站数量较上月有所增长，其他各类网络安全事件数量均有不同程度的下降。总体上，4月公共互联网网络安全态势较上月有所好转，评价指数在良的区间。

◆ 基础网络安全

2018年4月，我国基础网络运行总体平稳，互联网骨干网各项监测指标正常，未出现省级行政区域以上的造成较大影响的基础网络运行故障，未发生较大以上网络安全事件。

◆ 重要联网信息系统安全

本月，监测发现境内政府网站被篡改的数量为52个，与上月的57个相比下降8.8%，占境内被篡改网站的比例由2.2%上升到2.8%；境内政府网站被植入后门的数量为82个，与上月的73个相比增长12.3%，占境内被植入后门网站的比例由2.6%下降到2.5%；针对境内网站的仿冒页面数量为3,440个，较上月的3,791个下降9.3%。国家信息安全漏洞共享平台（CNVD^①）共协调处置了1,375起涉及我国政府部门以及银行、民航等重要信息系统部门以及电信、传媒、公共卫生、教育等相关行业的漏洞事件。

注①：CNVD是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库，致力于建立国家统一的信息安全漏洞收集、发布、验证、分析等应急处理体系。

◆ 公共网络环境安全

2018年4月，根据CNCERT的监测数据和通信行业报送数据，我国互联网网络安全环境主要指标情况如下：

网络病毒^②活动情况方面，境内感染网络病毒的终端数为近85万个，较上月增长12.9%；各安全企业报送的恶意代码捕获数量中，瑞星公司截获的病毒数量较上月下降2.4%，新增病毒数量较上月下降0.7%；安天公司捕获的样本总数较上月下降3.7%，新增病毒种类较上月下降8.8%；猎豹移动报送的计算机病毒事件数量较上月下降10.3%。

网站安全方面，境内被篡改网站数量为1,866个，较上月下降27.1%；境内被植入后门的网站数量为3,280个，较上月增长14.8%；针对境内网站的仿冒页面有3,440个，较上月下降9.3%；各安全企业报送的网页挂马情况中，奇虎360公司报送的网页挂马事件数量与上月持平。

安全漏洞方面，本月CNVD共收集整理信息系统安全漏洞1,130个，较上月下降40.6%。其中高危漏洞374个，较上月下降37.5%；可被利用来实施远程攻击的漏洞有992个，较上月下降39.2%。

事件受理方面，CNCERT接收到网络安全事件报告8,822件，较上月下降了8.6%，数量最多的分别是网页仿冒类事件3,040件、漏洞类事件2,617件。

事件处理方面，CNCERT处理了网络安全事件8,829件，数量最多的分别是网页仿冒类事件3,051件、漏洞类事件2,614件。

注②：一般情况下，恶意代码是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。其中，网络病毒是特指有网络通信行为的恶意代码。1月，CNCERT在对恶意代码进行抽样监测时，对545种木马家族和80种僵尸程序家族进行了抽样监测。

本月重点网络安全信息

◆ 2018 年网络安全威胁治理峰会暨 2017 年我国互联网网络安全态势报告发布会在京召开

4 月 25 日，国家互联网应急中心在京举办了 2018 年网络安全威胁治理峰会暨 2017 年我国互联网网络安全态势报告发布会。来自政府部门、重要信息系统单位、电信运营企业、域名注册管理和服务机构、行业协会、互联网和安全企业、应用商店等 80 多家单位的专家和代表出席了会议。

中央网信办网络安全协调局胡啸副局长、工业和信息化部网络安全管理局梁斌副局长等相关部门领导出席会议并致辞。胡啸副局长强调，要认真贯彻落实习总书记重要讲话精神，进一步做好网络安全工作，一是要加强网络安全风险报告、情报共享、分析研判，二是不断完善政府和企业网络安全信息共享机制，三是加强网络威胁源头治理，四是继续深入开展网络安全宣传教育。梁斌副局长肯定了 CNCERT 在网络安全事件监测发现、预警通报和协调处置等方面取得的成绩，介绍了通信行业为保障网络安全所做的主要工作。CNCERT 云晓春副主任介绍了中国互联网网络安全威胁治理联盟（CCTGA）成立至今发展情况和近年来在网络安全威胁治理方面的工作情况。

会议围绕以下内容进行了全面地介绍和交流：

一是发布了《2017 年我国互联网网络安全态势报告》。该报告基于 CNCERT 统计数据，结合日常应急处置工作实践编撰而成，介绍了我国境内木马僵尸网络、网页篡改、网站后门、网络仿冒、移动互联网恶意程序、安全漏洞等统计数据，分析总结了 2017 年我国网络安全的形势特点和 2018 年值得关注的热点问题。CNCERT 希望该报告能对政府机构、重要信息系统部门、行业单位和社会公众了解掌握当前网络安全形势和主要威胁、提高网络安全防护意识有所帮助。

二是探讨了威胁治理联盟发展思路 and 方案。CNCERT 作为联盟工作秘书处，提出本年度将从以下四个层面推进联盟发展：（一）继续推进网络安全威胁情报共享和网络安全威胁治理工作；（二）在可控环境内开放网络安全数据测试环境，帮助安全企业提升在网络流量分析、恶意样本分析等方面的技术能力；（三）建设国内 CERT 社群，帮助国内企业建设网络安全应急响应机制，协助国内安全企业走向国际；（四）设立“CCTGA 专业工作组”，推进网络安全威胁的专业化治理工作，并就安恒、华为、洋浦伟业等公司的提出的成立“网络安全威胁情报共享”、“DDoS 攻击威胁治理”、“移动互联网恶意程序治理”等专业方向工作组的建议进行了讨论。

三是举办威胁治理联盟成员单位表彰仪式。会上，总结了威胁治理联盟在网络安全威胁情报共享、分析和治理工作情况，公布了 2018 年新获准加入联盟的 15 家成员单位名单，并对在威胁治理工作中表现突出的 14 家联盟成员单位进行了表彰。

四是介绍 2018 年中国网络安全年会筹备情况。由 CNCERT 主办的、一年一度的中国网络安全年会将于 2018 年 8 月 14 日至 16 日在北京国家会议中心举办，本次会上介绍了会议筹备情况以及将与之同期举办的 2018 年中国网络安全技术对抗赛基本情况。

◆ 通报一例境外滥用我国境内网络资源发起大规模 DDoS 攻击的事件分析

4 月，CNCERT 监测发现 1900 端口在 4 月 10 日出现多次流出方向流量暴增的情况，峰值流量超过 800Gbps，疑似出现大规模 DDoS 攻击事件。经分析，发现两个境外 IP 地址收到了来自境内大量服务器 1900 端口的 UDP 反射攻击。从供给流量的时序来看，两个被攻击 IP 的攻击流量形态极为相似，由此可见，可能为统一组织对两个 IP 发起的攻击。此次 DDoS 反射攻击伪造被攻击 IP 地址向反射服务器的 1900 端口发起 UDP 请求，通过反射服务器向被攻击 IP 返回放大

的流量来对被攻击 IP 实施攻击。因此，以被攻击 IP 为源地址的流量来源能反映其真实的攻击来源。本次通过伪造被攻击 IP 地址的发起流量来源基本都位于境外，占全部伪造被攻击 IP 地址发起流量的 95% 以上。由此可见，该大规模流量攻击事件系境外方向滥用我国境内网络资源发起的网络攻击。这一事件也表明，我国应加强境内服务器的安全防护工作，关闭不必要的服务端口，加强对客户流量的审计，避免被攻击者滥用于恶性网络攻击。

◆ 通报 WebLogic Server WLS 核心组件存在反序列化漏洞

4 月，CNVD 收录了 WebLogic Server WLS 核心组件反序列化漏洞^③。攻击者利用该漏洞，可在未授权的情况下远程执行代码。漏洞验证代码已被公开，近期被不法分子利用进行大规模攻击的可能性较大，厂商已发布补丁进行修复。CNVD 对该漏洞的综合评级为“高危”。临时修复建议：通过设置 `weblogic.security.net.ConnectionFilterImpl` 默认连接筛选器，对 T3/T3s 协议的访问权限进行配置，阻断漏洞利用途径。美国甲骨文公司已发布了修复补丁，建议及时更新至最新版本：<http://www.oracle.com/technetwork/security-advisory/cpuapr2018-3678067.html>。

◆ 通报 Drupal 核心远程代码执行漏洞

4 月，CNVD 收录了 Drupal 核心远程代码执行漏洞^④。综合利用上述漏洞，攻击者可实现远程代码执行攻击。部分漏洞验证代码已被公开，近期被不法分子利用进行大规模攻击的可能性较大，厂商已发布补丁进行修复。CNVD 对上述漏洞的综合评级为“高危”。目前，厂商已发布补丁和安全公告以修复该漏洞，具体修复建议如下：Drupal 7.x 请升级到 Drupal 7.59 版本。同时官方给出 7.X 版本补丁，若用户无法立即升级版本，请更新补丁，补丁地址为：

注③：CNVD-2018-07811，对应 CVE-2018-2628。

注④：CNVD-2018-08523，对应 CVE-2018-7602。

<https://cgit.drupalcode.org/drupal/rawdiff/?h=7.x&id=080daa38f265ea28444c540832509a48861587d0>

本月网络安全主要数据

◆ 网络病毒监测数据分析

2018年4月，境内感染网络病毒的终端数为近85万个。其中，境内近64万个IP地址对应的主机被木马或僵尸程序控制，与上月的42万余个相比增长50.5%。

➤ 木马僵尸网络监测数据分析

2018年4月，境内近64万个IP地址对应的主机被木马或僵尸程序控制，按地区分布感染数量排名前三位的分别是浙江省、河南省、广东省。

木马或僵尸网络控制服务器IP总数为75,198个。其中，境内木马或僵尸程序控制服务器IP有18,331个，按地区分布数量排名前三位的分别为广东省、湖南省、浙江省。境外木马或僵尸程序控制服务器IP有56,867个，主要分布于美国、中国香港、日本。其中，位于美国的控制服务器控制了境内295,723个主机IP，控制境内主机IP数量居首位，其次是位于加拿大和中国香港的IP地址，分别控制了境内57,352个和54,945个主机IP。

➤ 网络病毒捕获和传播情况

网络病毒主要针对一些防护比较薄弱，特别是访问量较大的网站通过网页挂马的方式进行传播。当存在安全漏洞的用户主机访问了这些被黑客挂马的网站后，会经过多级跳转暗中连接黑客最终“放马”的站点下载网络病毒。2018年4月，CNCERT监测发现排名前十的活跃放马站点域名和活跃放马站点IP如表1所示。

表 1 2018 年 4 月活跃放马站点域名和 IP

排序	活跃放马站点域名	排序	活跃放马站点 IP
1	download.glzip.cn	1	182.140.228.250
2	der.kuai-go.com	2	92.23.61.109
3	ossi4.51cto.com	3	111.230.128.148
4	www.45ik.com	4	219.153.17.122
5	dl.360safe.com	5	219.159.249.122
6	elhoumaupload.com	6	123.207.27.171
7	r.kuai-go.com	7	119.29.183.196
8	neirong.funshion.com	8	183.131.155.242
9	www.courtneymorehead.com	9	139.199.16.78
10	asedownloadgate.com	10	123.207.116.121

网络病毒在传播过程中，往往需要利用黑客注册的大量域名。2018 年 4 月，CNCERT 监测发现的放马站点中，通过域名访问的共涉及有 546 个域名，通过 IP 直接访问的共涉及有 77 个 IP。在 546 个放马站点域名中，于境内注册的域名数为 201 个（约占 36.8%），于境外注册的域名数为 124 个（约占 22.7%）。放马站点域名所属顶级域名排名前 5 位的具体情况如表 2 所示。

表 2 2018 年 4 月活跃恶意域名所属顶级域名

排序	顶级域名 (TLD)	类别	恶意域名数量
1	.COM	通用顶级域名 (gTLD)	221
2	.CN	国家顶级域名 (ccTLD)	144
3	.LOAN	通用顶级域名 (gTLD)	32
4	.NET	通用顶级域名 (gTLD)	20
5	.ORG	通用顶级域名 (gTLD)	14

◆ 网站安全数据分析

➤ 境内网站被篡改情况

2018 年 4 月，境内被篡改网站的数量为 1,866 个，境内被篡改网站数量按地区分布排名前三位的分别是广东省、北京市、浙江省。按网

站类型统计，被篡改数量最多的是.COM 域名类网站，其多为商业类网站；值得注意的是，被篡改的.GOV 域名类网站有 52 个，占境内被篡改网站的比例为 2.8%。

➤ 境内网站被植入后门情况

2018 年 4 月，境内被植入后门的网站数量为 3,280 个，境内被植入后门的网站数量按地区分布排名前三位的分别是广东省、北京市、河南省。按网站类型统计，被植入后门数量最多的是.COM 域名类网站，其多为商业类网站；值得注意的是，被植入后门的.GOV 域名类网站有 82 个，占境内被植入后门网站的比例为 2.5%。

2018 年 4 月，境外 2,875 个 IP 地址通过植入后门对境内 3,280 个网站实施远程控制。其中，境外 IP 地址主要位于美国、中国香港和俄罗斯等国家或地区。从境外 IP 地址通过植入后门控制境内网站数量来看，来自中国香港的 IP 地址共向境内 640 个网站植入了后门程序，入侵网站数量居首位；其次是来自美国和乌克兰的 IP 地址，分别向境内 501 个和 445 个网站植入了后门程序。

➤ 境内网站被仿冒情况

2018 年 4 月，CNCERT 共监测到针对境内网站的仿冒页面有 3,440 个，涉及域名 1,481 个，IP 地址 430 个，平均每个 IP 地址承载 8 个仿冒页面。在这 430 个 IP 中，98.6% 位于境外，主要位于中国香港和美国。

◆ 漏洞数据分析

2018 年 4 月，CNVD 收集整理信息系统安全漏洞 1,130 个。其中，高危漏洞 374 个，可被利用来实施远程攻击的漏洞有 992 个。受影响的软硬件系统厂商包括 Adobe、Cisco、Drupal、Google、IBM、Linux、Microsoft、Mozilla、WordPress 等。

根据漏洞影响对象的类型，漏洞可分为操作系统漏洞、应用程序

漏洞、WEB 应用漏洞、数据库漏洞、网络设备漏洞（如路由器、交换机等）和安全产品漏洞（如防火墙、入侵检测系统等）。本月 CNVD 收集整理的漏洞中，按漏洞类型分布排名前三位的分别是应用程序漏洞、WEB 应用漏洞、操作系统漏洞。

◆ 网络安全事件接收与处理情况

➤ 事件接收情况

2018 年 4 月，CNCERT 收到国内外通过电子邮件、热线电话、网站提交、传真等方式报告的网络安全事件 8,822 件（合并了通过不同方式报告的同一网络安全事件，且不包括扫描和垃圾邮件类事件），其中来自国外的事件报告有 50 件。

在 8,822 件事件报告中，排名前三位的安全事件分别是网页仿冒、漏洞、恶意程序。

➤ 事件处理情况

对国内外通过电子邮件、热线电话、传真等方式报告的网络安全事件，以及自主监测发现的网络安全事件，CNCERT 每日根据事件的影响范围和存活性、涉及用户的性质等因素，筛选重要事件进行协调处理。

2018 年 4 月，CNCERT 以及各省分中心共同协调处理了 8,829 安全事件。其中网页仿冒、漏洞类事件处理数量较多。

附：术语解释

● 信息系统

信息系统是指由计算机硬件、软件、网络和通信设备等组成的以处理信息和数据为目的的系统。

● 漏洞

漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险。

● 恶意程序

恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序。恶意程序分类说明如下：

1. 特洛伊木马 (Trojan Horse)

特洛伊木马 (简称木马) 是以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意代码。由于它像间谍一样潜入用户的电脑，与战争中的“木马”战术十分相似，因而得名木马。按照功能，木马程序可进一步分为：盗号木马^⑤、网银木马^⑥、窃密木马^⑦、远程控制木马^⑧、流量劫持木马^⑨、下载者木马^⑩和其它木马七类。

2. 僵尸程序 (Bot)

僵尸程序是用于构建大规模攻击平台的恶意代码。按照使用的通信协议，僵尸程序可进一步分为：IRC 僵尸程序、Http 僵尸程序、P2P 僵尸程序和其它僵尸程序四类。

3. 蠕虫 (Worm)

蠕虫是指能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意代码。按照传播途径，蠕虫可进一步分为：邮件蠕虫、即时消息蠕

注⑤：盗号木马是用于窃取用户电子邮箱、网络游戏等账号的木马。

注⑥：网银木马是用于窃取用户网银、证券等账号的木马。

注⑦：窃密木马是用于窃取用户主机中敏感文件或数据的木马。

注⑧：远程控制木马是以不正当手段获得主机管理员权限，并能够通过网络操控用户主机的木马。

注⑨：流量劫持木马是用于劫持用户网络浏览的流量到攻击者指定站点的木马。

注⑩：下载者木马是用于下载更多恶意代码到用户主机并运行，以进一步操控用户主机的木马。

虫、U 盘蠕虫、漏洞利用蠕虫和其它蠕虫五类。

4. 病毒 (Virus)

病毒是通过感染计算机文件进行传播,以破坏或篡改用户数据,影响信息系统正常运行为主要目的恶意代码。

5. 其它

上述分类未包含的其它恶意代码。

随着黑客地下产业链的发展,互联网上出现的一些恶意代码还具有上述分类中的多重功能属性和技术特点,并不断发展。对此,我们将按照恶意代码的主要用途参照上述定义进行归类。

- 僵尸网络

僵尸网络是被黑客集中控制的计算机群,其核心特点是黑客能够通过一对多的命令与控制信道操纵感染木马或僵尸程序的主机执行相同的恶意行为,如可同时对某目标网站进行分布式拒绝服务攻击,或发送大量的垃圾邮件,或进行“挖矿”等。

- 拒绝服务攻击

拒绝服务攻击是向某一目标信息系统发送密集的攻击包,或执行特定攻击操作,以期致使目标系统停止提供服务。

- 网页篡改

网页篡改是恶意破坏或更改网页内容,使网站无法正常工作或出现黑客插入的非正常网页内容。

- 网页仿冒

网页仿冒是通过构造与某一目标网站高度相似的页面(俗称钓鱼网站),并通常以垃圾邮件、即时聊天、手机短信或网页虚假广告等方式发送声称来自于被仿冒机构的欺骗性消息,诱骗用户访问钓鱼网站,以获取用户个人秘密信息(如银行帐号和帐户密码)。

- 网页挂马

网页挂马是通过在网页中嵌入恶意代码或链接,致使用户计算机在访问该页面时被植入恶意代码。

- 网站后门

网站后门事件是指黑客在网站的特定目录中上传远程控制页面从而能够通

过该页面秘密远程控制网站服务器的攻击事件。

- 垃圾邮件

垃圾邮件是将不需要的消息（通常是未经请求的广告）发送给众多收件人。包括：（一）收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件；（二）收件人无法拒收的电子邮件；（三）隐藏发件人身份、地址、标题等信息的电子邮件；（四）含有虚假的信息源、发件人、路由等信息的电子邮件。

- 域名劫持

域名劫持是通过拦截域名解析请求或篡改域名服务器上的数据，使得用户在访问相关域名时返回虚假 IP 地址或使用户的请求失败。

- 非授权访问

非授权访问是没有访问权限的用户以非正当的手段访问数据信息。非授权访问事件一般发生在存在漏洞的信息系统中，黑客利用专门的漏洞利用程序（Exploit）来获取信息系统访问权限。

- 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。