# 国家计算机病毒应急处理中心监测发现20余款违规移动应用

汇报人：

2024-01-15

# 目录

# 01

# 引言

# 背景介绍

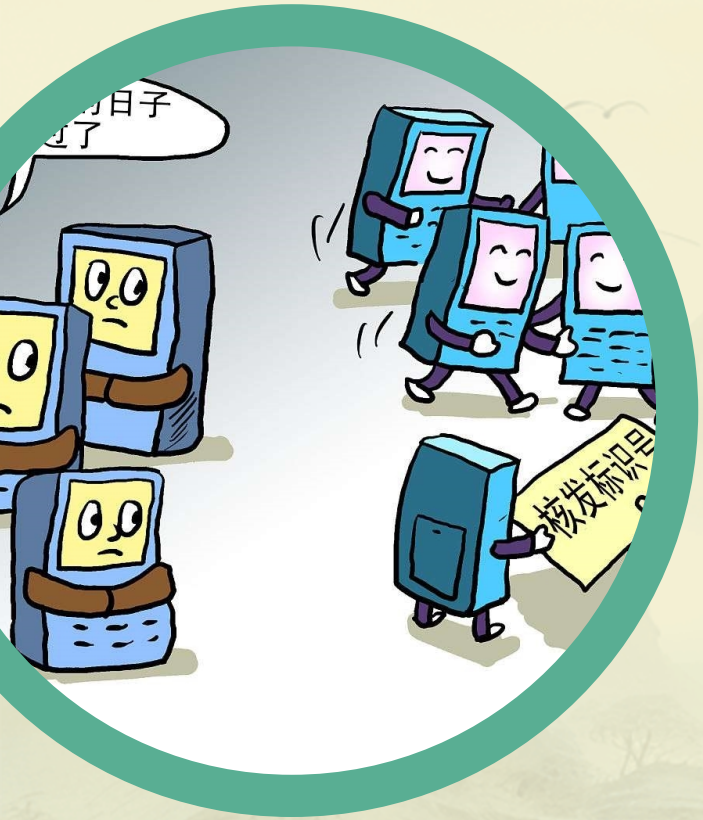

## 移动互联网的普及

随着移动互联网的快速发展，移动应用成为人们日常生活中不可或缺的一部分。然而，一些不法分子利用移动应用进行恶意行为，给用户带来安全隐患。

## 国家计算机病毒应急处理中心的职责

国家计算机病毒应急处理中心是负责监测、预警、处置计算机病毒和恶意软件的权威机构，旨在维护国家信息安全和公民个人信息安全。

# 违规移动应用概述




## 违规移动应用的定义

违规移动应用是指那些违反国家法律法规、侵犯用户权益、传播恶意代码或进行其他非法活动的移动应用。

## 违规移动应用的危害

违规移动应用可能导致用户隐私泄露、财产损失、设备性能下降等问题，甚至对国家安全和社会稳定造成威胁。

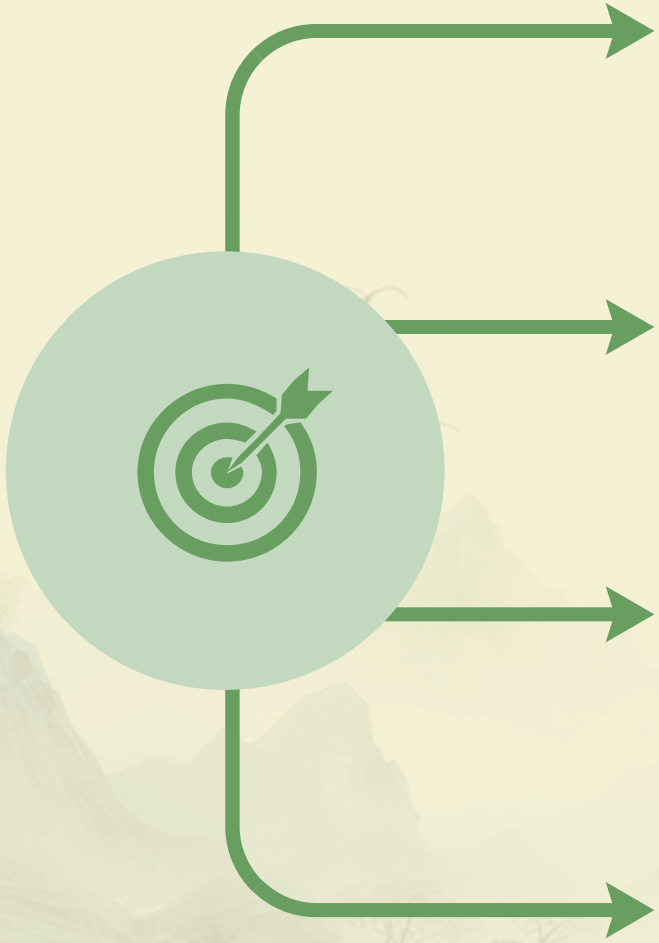
## 国家计算机病毒应急处理中心的监测结果

近期，国家计算机病毒应急处理中心在监测中发现20余款违规移动应用，这些应用涉及多个领域，包括游戏、社交、工具等。

# 02

# 违规移动应用分析

# 违规类型



## 恶意扣费

部分应用通过隐藏执行、欺骗用户点击等手段，在用户不知情的情况下进行恶意扣费。

## 隐私窃取

一些应用私自收集用户个人信息，如通讯录、短信、照片等，严重侵犯用户隐私。

## 诱骗欺诈

部分应用通过伪造虚假信息、冒充官方机构等手段，诱导用户进行转账、汇款等操作，实施网络诈骗。

## 恶意传播

一些应用自身携带病毒或恶意代码，通过自动下载、安装其他应用或传播恶意链接等方式，造成用户设备感染病毒或遭受攻击。

# 危害程度

## 经济损失

恶意扣费类应用直接导致用户经济损失，且由于扣费行为隐蔽，用户往往难以及时发现并挽回损失。

## 隐私泄露

隐私窃取类应用将用户个人信息泄露给不法分子，可能导致用户遭受电话骚扰、网络诈骗等更严重的后果。

## 信任危机

诱骗欺诈类应用利用用户对官方机构的信任，实施诈骗行为，严重损害用户对官方机构的信任度。

## 安全威胁

恶意传播类应用不仅危害用户设备安全，还可能通过传播恶意代码、发起网络攻击等行为，对整个网络安全造成威胁。

# 传播途径

## 应用商店

部分违规应用通过伪装成正规应用或利用应用商店审核漏洞等方式，上传至应用商店供用户下载。

## 社交媒体

一些违规应用通过社交媒体平台发布虚假广告或诱导性链接，吸引用户点击并下载安装。

## 恶意网站

部分违规应用通过恶意网站进行传播，用户在访问这些网站时可能会被诱导下载并安装违规应用。

## 二维码传播

一些违规应用将自身伪装成正规应用的二维码，在公共场所或网络上发布，用户扫描后可能会自动下载并安装违规应用。

# 03

# 监测与发现过程

# 监测方法

1

## 基于大数据的实时监测

利用先进的大数据技术，对国家范围内的计算机网络进行24小时不间断的实时监测，捕捉异常流量和行为模式。

2

## 静态代码分析

通过对移动应用进行反编译和静态代码分析，检测其中是否存在恶意代码、违规收集用户信息等行为。

3

## 动态行为分析

在沙箱环境中运行移动应用，观察其行为并进行记录和分析，以发现潜在的安全威胁和违规行为。

# 发现过程

## 异常流量筛选

在实时监测过程中，对异常流量进行筛选和分析，确定可能存在问题的移动应用。

## 问题应用定位

通过静态代码分析和动态行为分析，对问题应用进行深入分析，确定其违规行为和性质。

## 样本获取与验证

获取问题应用的样本，并在安全实验室环境中进行验证和复现，确保结果的准确性和可靠性。

# 数据分析

## 数据统计与可视化

对监测数据进行统计和可视化处理，直观地展示移动应用的安全状况和违规行为的分布情况。

## 关联分析与挖掘

利用关联分析算法，挖掘违规移动应用之间的关联关系和潜在的安全威胁。

## 趋势分析与预测

通过对历史数据的分析，预测未来可能出现的新的违规行为和安全威胁，为防范和应对提供决策支持。