



National Cyber Security Centre

a part of GCHQ



Australian Government  
Australian Signals Directorate

**ASD** AUSTRALIAN SIGNALS DIRECTORATE  
ACSC Australian Cyber Security Centre



Bundesamt für Verfassungsschutz



Communications Security Establishment

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications

Centre canadien pour la cybersécurité



National Cyber Security Centre

PART OF THE GCSB



# 公告

## BADBAZAAR 和 MOONSHINE:

针对维吾尔族人、台湾人和藏人团体以及民间社会活动者的间谍软件



2025 年 4 月 9 日

# BADBAZAAR 和 MOONSHINE：针对维吾尔人、台湾人和藏人团体以及民间社会活动者的间谍软件

英国国家网络安全中心（**NCSC**）及其合作伙伴联合发布公告，公布了针对两种间谍软件变种的最新情报和缓解措施，重点面向面临高风险的群体。

## 概要

---

本公告是在英国 [网络联盟（Cyber League）](#) 的支持下，由英国国家网络安全中心（National Cyber Security Centre，简称 NCSC UK）和国际合作伙伴联合发布：

- › 澳大利亚网络安全中心，隶属于澳大利亚信号局
- › 加拿大网络安全中心，隶属于通信安全机构
- › 德国联邦情报局
- › 德国联邦宪法保卫局
- › 新西兰国家网络安全中心，隶属于政府通信安全局
- › 美国联邦调查局
- › 美国国家安全局

恶意网络行为者对与台湾、西藏、新疆维吾尔自治区、民主运动和法轮功等议题相关的个人构成了日益严重的威胁，本公告旨在提高公众对这一情况的认识。

本公告包含两个案例研究，详细介绍了恶意网络行为者如何使用名为 **BADBAZAAR** 和 **MOONSHINE** 的间谍软件，针对包括智能手机在内的移动设备中的数据进行了攻击，这些数据可能引起中国政府的兴趣。本公告还指引了相关建议，帮助个人保护自身及其设备和数据安全。

除此公告外，NCSC 还另行发布了 [完整技术细节和配套指南](#)。

## 谁面临风险？

---

本公告编制机构及其行业合作伙伴观察到，BADBAZAAR 和 MOONSHINE 专门针对与中国政府认为威胁其在国内的权威、国家目标和国际声誉的议题相关的个人。面临攻击风险最大的人群包括（但不限于）与以下议题有关的任何人士：

- › 台湾独立
- › 西藏人权
- › 中国新疆维吾尔自治区境内或来自新疆维吾尔自治区的维吾尔族穆斯林及其他少数民族
- › 民主倡议（包括香港）
- › 法轮功精神运动

这包括倡导、认同或以其他方式代表上述群体的非政府组织（NGO）、记者、企业和个人。这种间谍软件在网上的传播方式具有非定向性，这也意味着其感染范围可能超出目标人群。

本公告旨在帮助面临风险的群体有效应对 BADBAZAAR 和 MOONSHINE 间谍软件所带来的特定威胁。所建议的缓解措施是对更广泛的网络安全建议的补充，不应被孤立使用。

通过遵循本公告中提及的指南，用户可以降低其移动设备和数据受到感染的风险。

## 威胁概述

---

MOONSHINE 和 BADBAZAAR 是一种木马病毒；其恶意功能隐藏在可从应用商店或在线文件共享服务下载的表面上正常运行的应用程序中。

这些应用程序旨在诱导用户在设备上下载并安装它们。一旦应用程序得到安装后，就会利用设备上的漏洞执行未经授权的功能，或者可能依赖用户授予的应用程序权限来访问和下载设备中的信息，包括：

- › 位置数据（包括实时定位）
- › 访问麦克风和摄像头
- › 设备上存储的短信、照片和其他文件
- › 设备信息等

攻击者然后会利用目标群体的合法利益，以识别并感染尽可能多的受害者，并获取他们的数据。他们为此采取的手法之一就是设计迎合受害者群体偏好的应用程序，如支持其母语或者含有与地区（如中国西藏地区或新疆）相关内容的应用程序。

本公告中的案例研究提供了这方面的一些例子，包括 TibetanOne 和《维吾尔古兰经》（Uyghur Quran）应用程序。

恶意网络行为者活跃于拥有目标受害者用户群的在线论坛，最大限度地增加了感染受害者的机会。据观察，他们故意在与西藏相关的 Telegram 频道和 Reddit 论坛上分享间谍软件。本公告中的案例研究也提供了这些方法的例子。

恶意应用程序通常以独立文件（如 Android 上的 APK 文件）的形式分享，需要用户下载并安装。恶意网络行为者会尝试通过将间谍软件上传到官方应用商店（如 Google Play Store 和 Apple App Store），或者在原本无害的应用程序中植入恶意代码，使其看起来更合法。但官方商店具有安全机制和审查流程，使得这种策略的成功率较低。这就使得来自官方商店的应用程序更加安全，但正如案例研究和 NCSC 的 [《应用程序商店威胁报告》（App Store Threat Report）](#) 所示，这些机制并非完美无缺。

遵循以下 4 项建议，有助于防范本公告中所述的威胁。

有关更详细的建议，请参阅缓解措施部分。



# Four tips to stay safe when using your smartphone

Reduce the risk from malicious apps with good cyber hygiene, then follow these four principles:

## Stay Mainstream >

Don't root or jailbreak devices, only use trusted app stores.



## Stay Organised >

Review installed apps and permissions regularly.



## Stay in Touch >

Report suspicious messages and files to online services.



## Stay Alert >

Stay vigilant on social media and check shared files and links.



## 案例研究

---

这两个案例研究说明了 MOONSHINE 和 BADBAZAAR 的运作方法，以及恶意网络行为者如何针对那些风险最高的人群进行攻击。

### 案例研究一：MOONSHINE

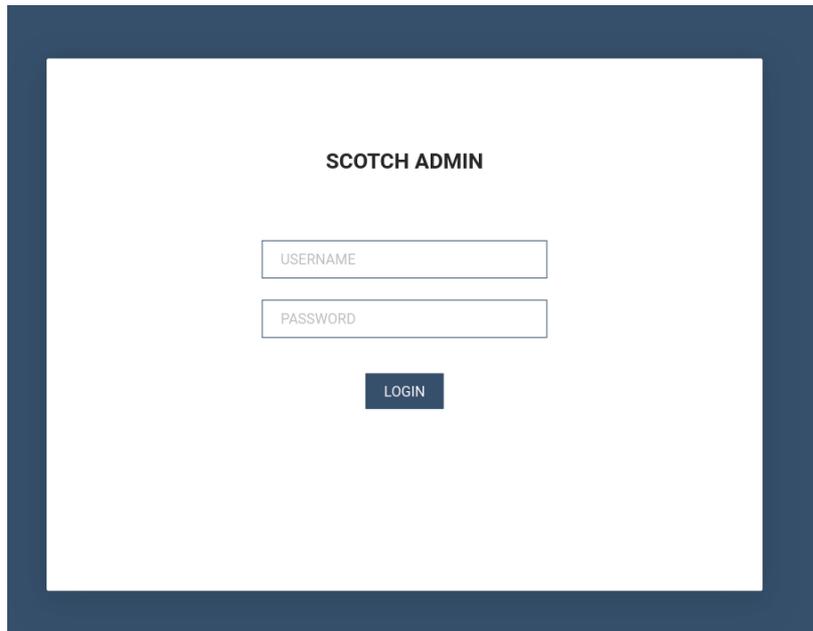
MOONSHINE 是一款针对藏人团体的 Android 间谍软件，由“公民实验室” ([Citizen Lab](#)) 于 2019 年披露。MOONSHINE 伪装成合法应用程序，诱导受害者进行安装。该应用程序通过 Telegram 频道和 WhatsApp 链接传播。

MOONSHINE 具有广泛的监控能力，如：

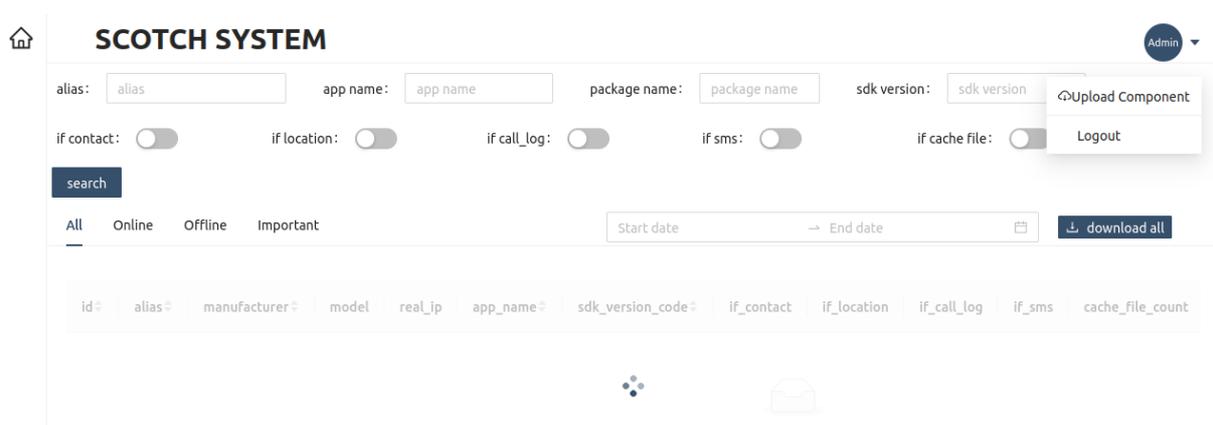
- › 位置数据（包括实时定位）
- › 实时录音和拍照
- › 从设备下载文件
- › 检索设备信息
- › 在设备上播放音频

名为“[ئاۋازلۇق قۇرئان .apk](#),”（翻译为“**Audio Quran.apk**”）的应用程序就是 MOONSHINE 针对维吾尔族用户的一个例子。在文件名中使用维吾尔语，并暗示其为一款《古兰经》应用程序，很可能是为了吸引维吾尔族穆斯林用户下载安装。

一旦安装，恶意网络行为者就能够从受害者的设备收集信息。这些信息可通过“SCOTCH ADMIN”面板进行访问。



一旦登录，恶意网络行为者就可以访问以下截屏所示的页面。此页面显示受感染设备的详细信息，以及恶意网络行为者对这些设备所拥有的访问权限级别：



恶意软件管理面板显示所收集的数据，包括：

- > 对设备的访问权限级别
- > **SMS** 短信
- > 通话记录
- > 位置数据
- > 设备信息

NCSC 与 Cyber League 协作，基于[趋势科技（Trend Micro）的行业报告](#)，发现 MOONSHINE 的漏洞利用工具包与 HTML 标题中包含“UPSEC”的登录面板之间存在重叠。完整详细信息请见随附的技术公告。

根据[《情报在线》（Intelligence Online）](#)的信息，“UPSEC”指的是“四川电科网安科技有限公司”（“Sichuan Dianke Network Security Technology Co. Ltd”）。本公告编制机构未证实此说法。

## 案例研究二：BADBAZAAR

BADBAZAAR 是一款移动端恶意软件，这一恶意软件具有 iOS 和 Android 版本，并曾针对维吾尔人、藏人和台湾人发动攻击。该恶意软件通过社交媒体平台和官方应用商店传播。

根据[Lookout](#)和[Volexity](#)的报告，BADBAZAAR 曾通过名为“**TibetOne**”的应用程序，对藏人团体实施攻击。**TibetOne** 是一款由恶意行为者创建的 iOS 应用程序，能够访问设备信息和位置数据。它于 2021 年 12 月上传至 Apple App Store，但现已下架。为了进一步传播该恶意软件，恶意行为者还通过一个名为“**tibetanphone**”的 Telegram 频道，对该应用程序进行广告宣传。



为了增加该应用程序的合法性，恶意行为者还开发了一个名为“[tibetone\[.\]org](http://tibetone[.]org)”的网站，该网站自称“为热爱西藏文化的人们带来丰富优质的作品，让阅读成为一种新的生活方式”。



图3: [tibetone\[.\]org](http://tibetone[.]org) 的主页。

该图像已经过编辑，以使相关部分更加清晰。

该网站有一个文章页面，用户可以发表评论。电邮地址“[choekyi.wangmo@ignitetibet.net](mailto:choekyi.wangmo@ignitetibet.net)”所发布的评论据信是由恶意行为者控制的，并可能冒充“**Choekyi Wangmo**”，而被西藏人权与民主中心 (Tibetan Centre of Human Rights and Democracy) 列为支持西藏的抗议者。这可能是恶意行为者再次企图为该应用程序营造其真诚倡导西藏独立的假象。

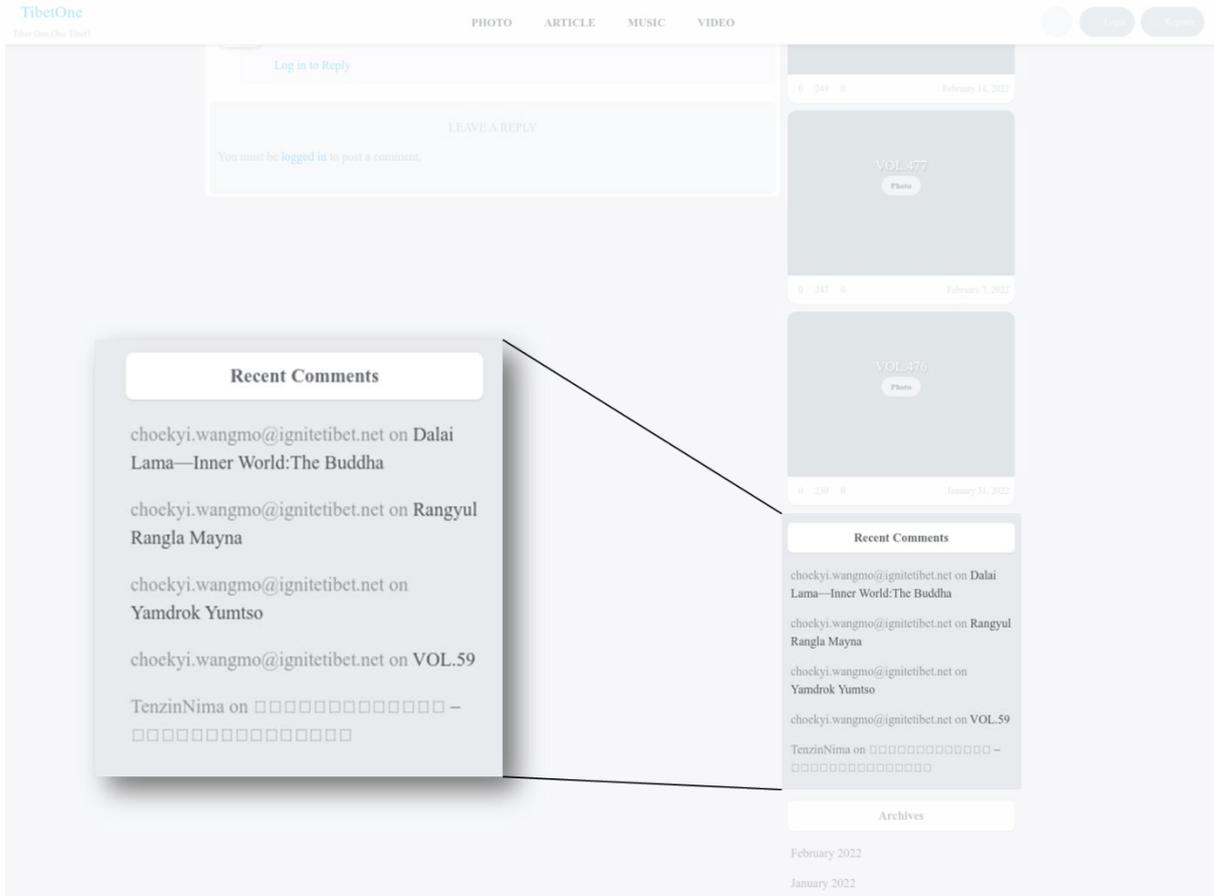


图4: tibetone[.]org 网站页面，显示疑似由恶意行为者控制的用户所发布的评论。

该图像已经过编辑，以使相关部分更加清晰。

“**TenzinNima**”是另一个在该网站发布评论的用户名。根据 [Volexity 的报告](#)，该用户名也在 Reddit 上用于宣传 Telegram 频道“**Tibetanmaptalk**”。其中包含一个链接，可用于下载恶意版本的“**AlpineQuest**”，是一款适用于 Android 设备的导航应用程序。所提供的下载链接指向一个名为 **Mega** 的第三方文件共享服务。

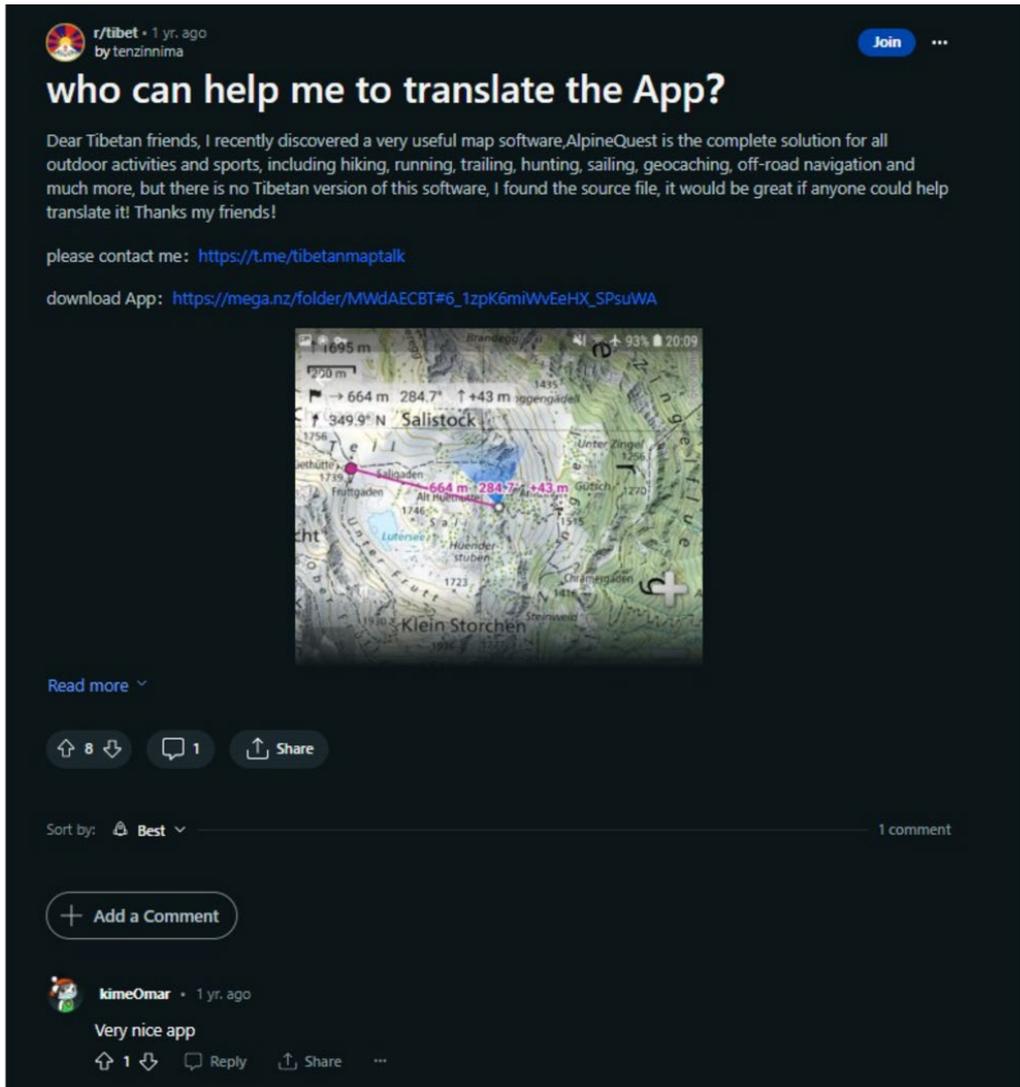


图5：疑似由恶意行为者控制的账户在 Reddit 上发布的恶意应用推广帖。

Volexity 还指出，有一位名为“**KimeOmar**”的用户曾在该帖文下发表评论，据观察，该用户还在另一个 Reddit 子论坛上分享恶意应用程序。这可能表明，恶意行为者使用多个社交媒体账户来使其帖子看起来更具可信度。

## 评估

---

BADBAZAAR 和 MOONSHINE 使用多种社会工程手段来专门针对维吾尔人、藏人和台湾人社区，包括：

- 对这些群体感兴趣的应用程序进行木马化，如维吾尔语《古兰经》应用程序，几乎可以肯定是针对目标受害者群体量身定制的
- 将这些木马化的应用程序上传到官方应用商店，很可能给人赋予其一定的合法性，并且在群聊中进行分享，极有可能是为了利用这些社区内部的信赖关系进行传播

BADBAZAAR 和 MOONSHINE 收集的数据几乎可以肯定对中国政府具有价值。尽管据目前观察，BADBAZAAR 和 MOONSHINE 一直针对维吾尔人、藏人和台湾人，但还有其他恶意软件针对中国其他少数民族群体。来自共同签章国家的公民（无论是在中国境内还是海外），若被视为威胁政权稳定事业的支持者，几乎可以肯定会面临来自 BADBAZAAR 和 MOONSHINE 等移动装置恶意软件的威胁。这些恶意软件具备获取位置、音频和照片数据的能力，几乎可以肯定会通过提供目标者的实时活动信息，来为未来的监视和骚扰行动提供情报支持的机会。

## 针对移动应用程序用户的缓解措施

本公告编制机构建议采取以下安全措施来防范案例研究中所述的威胁。这些建议以 NCSC 的最佳实践指南为基础。请参阅“延伸阅读”部分，获取有关澳大利亚和美国读者的最佳实践指南链接。

## 保持您的设备安全

- ▶ 仅从官方应用商店（如 **Google Play Store** 或 **Apple App Store**）下载应用程序。  
[Google Play Store](https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf) 和 [Apple App Store](https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf) 会在软件上线前对其进行病毒扫描，更能保障下载软件的安全性。来自受信任商店的应用程序仍可能存在风险，但从其他来源下载的应用程序可能根本没有任何安全保护。NCSC 有一份关于应用商店的威胁报告：  
<https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf>
- ▶ 保持您的设备和应用程序为最新版本。一旦应用程序和设备软件有更新可用，就应立即安装。如果可能的话，请在设备设置中启用“自动更新”，以免忘记手动操作。请参阅 NCSC 关于如何保持在线安全的指南，以防御已知病毒和其他类型的恶意软件的攻击。更新通常包括功能改进和新特性：  
<https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/install-the-latest-software-and-app-updates>
- ▶ 请勿对您的设备进行“越狱”或“root”（获取设备的最高管理员权限）操作，因为这会利用未修补的漏洞来绕过已实施的安全控制措施。这使得设备更容易受到攻击。请参阅 NCSC 指南：  
<https://www.ncsc.gov.uk/files/Threat-report-on-application-stores-web-v2.pdf>

## 管理您的应用程序

- › 检查您的应用程序及其权限设置。如果您不再需要某个应用，请将其删除。尽可能限制应用程序权限，最大限度地减少数据暴露的风险，因为恶意软件通常会专门访问受保护的文件或设备组件，如摄像头和麦克风。
  - Apple 用户查看应用权限的方法：  
<https://support.apple.com/en-gb/guide/iphone/iph251e92810/ios>
  - Android 用户查看应用权限的方法：  
<https://support.google.com/android/answer/9431959?hl=en-GB>
- › 自动将未知应用程序发送给 **Google** 检测。如果您是 Android 用户，并且下载了非来自 Google Play Store 的应用，可以通过启用 Google Play Store 中“Play Protect”设置下的“提升有害应用程序的检测能力”，将该应用程序发送给 Google。这将扫描应用程序来检测恶意软件，从而帮助保护用户。关于如何设置这一功能，请查阅：<https://support.google.com/android/answer/2812853?hl=en-GB>

## 使用网络安全服务

- › 在点击链接之前，请使用 **URL 信誉服务** 进行检查。您可以先使用 [Google Transparency Report](#)（《Google 透明度报告》）或 [Virus Total](#) 等服务来扫描来自电子邮件、短信或其他地方的链接，以检查其是否安全。您还可以将可疑文件和应用程序上传到恶意软件分析器（如 Virus Total），这些分析器可以帮助检测文件是否为恶意文件。请注意，扫描服务可能存在“漏报”（false negative）的情况。
- › 注册 **Google 高级保护（Google Advanced Protection）** 计划。这是一项免费服务，旨在保护使用 Google 服务（Gmail、Play Store 等）的高风险用户免受网络攻击。此项计划为使用 Google 服务的用户提供更高的安全性：  
<https://landing.google.com/advancedprotection/>
- › 注册额外的网络韧性服务（如适用）。例如，英国的高风险人群可能有资格获得额外的防御服务，以帮助他们保障网络安全。请查看资格并了解更多信息：

[https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section\\_7e](https://www.ncsc.gov.uk/collection/defending-democracy/guidance-for-high-risk-individuals#section_7e)

## 报告威胁行为

- › **识别并举报虚假账户。** 恶意网络行为者会创建虚假账户或入侵真实账户来达成其目的。如果您怀疑某个账户是虚假账户或者被盗账户，请向平台举报并将其屏蔽。许多服务都有验证账户的流程，例如 Instagram 和 Facebook 的“已验证徽章”。这可以帮助识别账户是否真实。NCSC 提供了关于安全使用社交媒体的指南，其中包括如何验证和举报被盗账户的详细信息：

<https://www.ncsc.gov.uk/guidance/social-media-how-to-use-it-safely>

- › **识别钓鱼邮件、短信和链接。** NCSC 可以调查可疑的电子邮件地址和网站。如果您认为某个网站、电子邮件或短信可疑，可以进行举报：

<https://www.ncsc.gov.uk/collection/phishing-scams>

# NCSC 术语表

---

## › Android

谷歌的移动操作系统，被多家智能手机和平板电脑制造商所采用。

## › 应用程序

应用程序（又称应用）是一种软件包，用户可以在设备上自行安装，或由设备预装，用于为设备提供额外的功能或内容。

## › 网络安全

保护设备、服务和网络以及其上的信息，以防止未经授权的访问、盗窃或损坏。

## › 设备

有实体形态的基于计算机的硬件，如台式计算机、智能手机或平板电脑。

## › iOS

Apple（苹果）在其一系列移动设备上使用的移动操作系统。

## › 恶意软件

恶意软件源自“恶意的软件”（英文“malicious software”），是指可能损害计算机系统、网络或设备的任何软件。包括病毒、勒索软件和木马程序。

## › 操作系统

在计算机、平板电脑和智能手机上运行、且支持其他应用程序和硬件运行所必需的基础软件。

## › 钓鱼攻击

诈骗电子邮件或短信，其中包含可能携带恶意软件的网站链接，或可能诱骗用户泄露敏感信息（如密码）或转账。

## › 间谍软件

一种未经用户同意安装在其设备上、收集数据然后将数据发送给第三方的恶意软件。

## › 社交媒体

允许人们分享和回应用户生成的内容（文本帖子、照片和视频）的网站和应用程序，如 Facebook、X 和 Instagram。

› **智能手机**

具备复杂功能的现代移动电话，包括运行 **Android** 和 **iOS** 操作系统的设备。

› **木马程序**

一种伪装成合法软件的恶意软件，用于获取对受害者的设备未经授权的访问权。

› **URL**

统一资源定位符。域名等万维网上的地址（如 **www.bbc.co.uk**）。

› **病毒**

一种旨在感染合法软件程序并在这些程序被激活时在整个网络进行复制传播的恶意软件。

## 延伸阅读

---

### 以下是澳大利亚网络安全中心的指南

- › [报告网络犯罪、事件或漏洞](#)
- › [如何保护您的设备安全](#)
- › [保护您的手机安全](#)
- › [钓鱼攻击](#)
- › [诈骗](#)
- › [保护您的社交媒体账户安全](#)
- › [社交媒体和通讯应用的安全建议](#)

### 以下是英国 NCSC 和 NPSA 的指南

- › [捍卫民主](#)
- › [社交媒体：如何安全使用](#)
- › [包括移动设备在内的组织设备安全指南](#)
- › [关于应用商店的威胁报告。](#)
- › [高风险个体的个人安全和安保](#)

### 以下是美国国家安全局（NSA）的指南

- › [移动设备最佳操作规范](#)

## 免责声明

---

请注意，本公告提供的信息在发布时已经过验证。

本报告借鉴了来自编制机构和行业渠道的信息。其中的任何调查结果及建议并非旨在完全规避所有风险，并且遵循这些建议也无法完全消除相关风险。信息风险的责任始终由相关系统的所有者承担。

在英国，本信息根据《2000 年信息自由法》（Freedom of Information Act 2000，简称 FOIA）被豁免公开，亦可能受其他英国信息立法的豁免条款保护。

如有任何 FOIA 相关查询，请发送电邮至 [ncscinfoleg@ncsc.gov.uk](mailto:ncscinfoleg@ncsc.gov.uk)。

所有材料均归英国皇家版权所有©

## 附件：已观察到的 MOONSHINE 和 BADBAZAAR 样本

下表列出了过去两年在 MOONSHINE 和 BADBAZAAR 行动中使用的应用程序。

其中许多应用程序与现有应用程序有明显的相似性。这很可能是恶意行为者故意“仿冒”知名品牌的手段。

务必要注意，应用程序的名称、软件包名称和图标都可能模仿或完全复制真实的应用程序，因此不能仅凭这些特征来判断设备是否被感染。

正如“缓解措施”部分所述，您可以通过启用“提升有害应用程序的检测能力”功能，将 Android 设备上的应用发送给 Google 进行扫描，以检测设备中从非 Play Store 安装的应用是否安全。

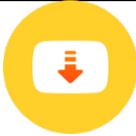
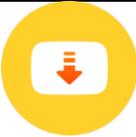
应用程序名称	软件包名称	应用程序图标
99 Names of ALLAH (真主的 99 个名字)	com.Apptriple.Namesofallah.Asmaulhusna	
APKPure	com.apkpure.aegon	
Adobe Acrobat	com.adobe.reader	
Alpine(بينتو)	psyberia.pa.full	
AlpineQuest Off-Road Explorer (AlpineQuest 越野探险者)	psyberia.alpinequest.full	
AlpineQuest Off-Road Explorer (AlpineQuest 越野探险者)	psyberia.alpinequest.full	

AlpineQuest Off-Road Explorer (Lite) (AlpineQuest 越野探险者 (精简版))	psyberia.alpinequest.free	
AppLock	com.alpha.applock	
Arabic Keyboard (阿拉伯语键盘)	com.arabic.keyboard.arabic.language.keyboard.app	
Audio Video Cutter (音视频剪辑器)	bsoft.com.mp3.cutter.ringtone.video.maker.trimmer	
Badam 维语输入法	com.ziipin.softkeyboard	
Buddhist Songs (1) (佛教歌曲 (1))	com.bigkidsapps.buddhistsongs1	
Calculator (计算器)	com.android2.calculator3	
Compass 360 Pro (指南针 360 专业版)	com.pro.app.compass	
EN-UG Dictionary Free (英语-维吾尔语词典免费版)	ru.vddevelopment.ref.enugen.free	
Ewlad	ewlat.com.ewlatuyghur	

FAST	com.netflix.Speedtest	
FMWhatsApp	com.fmwhatsapp	
File Manager + (文件管理器+)	com.alphainventor.filemanager	
FlyGram	org.telegram.FlyGram	
Flygram	org.telegram.FlyGram	
Free WiFi Pass (免费WiFi 通行证)	com.cl.wifipassword.share	
GBWhatsApp	com.gbwhatsapp	
Hefz Quran	com.golap.hefzquran	
Hijri Calendar (伊斯兰历)	com.ibrahim.hijricalendar	
InShot	com.camerasideas.instashot	

KMPlayer	com.kmplayer	
KineMaster	com.nexstreaming.app.kinemasterfree	
MP3 Cutter & Ringtone Maker (MP3 剪辑器和铃声制作器)	ringtone.maker.mp3.cutter.audio	
Malloc	com.mallocprivacy.antistalkerfree	
Maps Distance Calculator (地图距离计算器)	com.routemap.mapdownload.gpsrouteplanner	
Media Recovery (介质恢复)	com.aaa.media.recovery.androidapp	
Nur.cn	com.nur.reader	
Nur 输入法	com.nur.ime	
OGWhatsApp	com.gbwhatsapp3	
PDF Extra (PDF 附加版)	com.mobisystems.mobiscanner	

PDF Reader (PDF 阅读器)	pdf.pdfreader.pdfviewer.pdfeditor	
PDF Reader (PDF 阅读器)	com.gappstudios.autowifi3gdataswitch.san.basicpdfviewer	
Photo Editor (照片编辑器)	com.iudesk.android.photo.editor	
Photo Recovery (照片恢复)	recover.restore.undelete.photo.video.file	
Photo Studio (摄影工作室)	com.kvadgroup.photostudio	
Plus	org.telegram.pluspro	
Prayer Book (祈祷书)	com.arashpayan.prayerbook	
QuarkVPN	com.speedy.vpn	
Quran (古兰经)	com.tos.quranuighore	
QuranKerim (古兰经)	com.ewlat.qurankerim	
Restore Deleted Pics (删除照片恢复)	com.restore.deleted.pictures.video	

Signal (信号)	org.thoughtcrime.securesms	
Signal Plus (信号+)	org.thoughtcrime.securesmsplus	
Signal Plus (信号+)	org.thoughtcrime.securesmsplus	
Singing Bowl Sounds HD (颂钵音效 HD)	com.soundjabber.tibetansingingbowls. candletibet.bowlschakrasound	
Skype	com.skype.raider	
Snaptube	com.snaptube.premium	
Snaptube Plus	com.snaptube.gold	
SwiftKey Keyboard (SwiftKey 键盘)	com.touchtype.swiftkey	
Tarteel	com.mmmoussa.iqra	
Telegram	org.zhifeijihj.messenger	
Telegram	org.telegramfbo.messenger	

Telegram X	org.thunderdog.challegram	
Tibetan Divination System MO (西藏 MO 占卜系统)	rhombapp.mo	
Tibetan Prayer (藏语祈祷文)	com.chorig.tibetanprayer	
Translator AR-TR (阿拉伯语-土耳其语翻译器)	free_translator.artr	
Truecaller	com.truecaller	
TubePlus	com.techshop.videocraft	
Ultrasurf	us.ultrasurf.mobile.ultrasurf	
Uyghur Keyboard (维吾尔语键盘)	com.mykeyboard.myphotokeyboard.uyghurkeyboard	
Uyghurche Kirguzguch (维吾尔文输入法)	com.ziipin.softkeyboard	
Video Converter (视频转换器)	com.inverseai.video_converter	
Video Cutter (视频剪辑器)	com.naing.cutter	

Video Downloader (视频下载器)	downloader.video.download.free	
Video Maker (视频制作器)	com.bstech.slideshow.videomaker	
Video Player for Android (Android 视频播放器)	com.zgz.supervideo	
Vieka	com.prime.story.android	
VivaVideo Lite	com.quvideo.vivavideo.lite	
VivaVideo PRO	com.quvideo.xiaoying.pro	
Vmuslim	com.alhiwar	
Voice Recorder (录音机)	com.media.bestrecorder.audiorecorder	
Voxer	com.rebelvox.voxer	
Weather Forecast (天气预报)	com.graph.weather.forecast.channel	

WhatsApp	com.whatsapp	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp3Plus	
WhatsApp	com.whatsapp	
WhatsApp	com.WhatsApp2Plus	
Whoscall	gogolook.callgogolook2	
WiFi Password Master_v1.4	com.example.dat.a8andoserverx	
Windy	com.windyty.android	
Wise	com.transferwise.android	
YoWhatsApp	com.yowhatsapp	

YouTube Downloader (YouTube 下载器)	dentex.youtube.downloader	
Zom	im.zom.messenger	
iQuran Lite	com.guidedways.iQuran	
ئەسەرلەر ئاۋازلىق	com.ewlat.eserler	
قۇرئان ئاۋازلىق	com.c9.utilim	
ئىزچى	com.yelken.izchi	
ئىزدىگۈچى APK ئۇيغۇرچە	com.uygur.apkstore	
قۇرئان ئۇيغۇرچە	com.c9.uyghurquran	<b>قۇرئان</b>
الكريم القرآن	com.maher4web.quran	
زىكىرلەر	com.my.newproject5	
كەرىم قۇرئان	ru.omdevelopment.ref.quranuyghur.free	

لۇغىتى كۇھىقاپ	com.kuhiqap.lughitim	
كىرگۈزگۈچ نۇر	com.nur.ime	
《心灵法门》念佛机	com.guanyincitta.chant	
汉藏英辞典	com.dacd.dictionary	
藏历基本数据	com.example.astronomicalcalendarapp	
阳光藏汉翻译	com.tibetan.translate	