【电信安全】

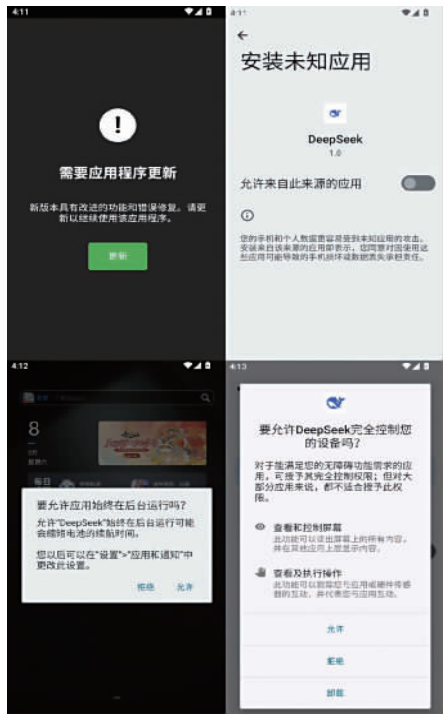
仿冒 DeepSeek 的手机木马病毒出现

近日，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室依托国家计算机病毒协同分析平台在我国境内捕获发现仿冒 DeepSeek 官方 App 的安卓平台手机木马病毒。

用户一旦点击运行仿冒 App，该 App 会提示用户 “需要应用程序更新”，并诱导用户点击“更新”按钮。用户点击后，会提示安装所谓的 “新版” DeepSeek 应用程序，实际上是包含恶意代码的子安装包，并会诱导用户授予其后台运行和使用无障碍服务的权限。

同时，该恶意 App 还包含拦截用户短信、窃取通讯录、窃取手机应用程序列表等侵犯公民个人隐私信息的恶意功能和阻止用户卸载的恶意行为。经分析，该恶意 App 为金融盗窃类手机木马病毒的新变种。网络犯罪分子很可能将该恶意 App 用于电信网络诈骗活动，诱使用户从非官方渠道安装仿冒 DeepSeek 的手机木马，从而对用户的个人隐私和经济利益构成较大威胁。

除仿冒 DeepSeek 安卓客户端的“DeepSeek.apk”之外，国家计算机病毒协同分析平台还发现了多个文件名为



“DeepSeek.exe”“DeepSeek.msi”和“DeepSeek.dmg”的病毒样本文件，由于 DeepSeek 目前尚未针对 Windows 平台和 MacOS 平台推出官方客户端程序，因此相关文件均为仿冒程序。由此可见，网络犯罪分子已经将仿冒 DeepSeek 作为传播病毒木马程序的新手法。预计未来一段时间内，包括仿冒 DeepSeek 在内的各种人工智能应用程序的病毒木马将持续增加。

国家计算机病毒应急处理中心发布防范措施

针对该款手机木马病毒，国家计算机病毒应急处理中心发布以下防范措施：

1、不要从短信、社交媒体软件、网盘等非官方渠道传播的网络链接或二维码下载 App，仅通过 DeepSeek 官方网站或正规手机应用商店下载安装相应 App。

2、保持手机预装的安全保护功能或第三方手机安全软件处于实时开启状态，并保持手机操作系统和安全软件更新到最新版本。

3、在手机使用过程中，谨慎处理非用户主动发起的 App 安装请求，一旦发现 App 在安装过程中发起对设备管理器、后台运行和使用无障碍功能等权限请求，应一律予以拒绝。

4、如遭遇安装后无法正常卸载的 App 程序，应立即备份手机中的通讯录、短信、照片、聊天记录和文档文件等重要数据，在手机生产商售后服务人员或专业人员的指导下对手机进行安全检测和恢复。同时密切关注本人的社交媒体类软件和金融类软件是否具有异常登录信息或异常操作信息，以及亲友是否收到由本人手机号或社交媒体软件发送的异常信息，一旦出现上述相关情况，应及时联系相关软件供应商和亲友说明有关情况。

5、警惕和防范针对流行 App 软件的电信网络诈骗话术，如“由于 XXX 软件官方网站服务异常，请通过以下链接下载官方应用程序”“由于 XXX 软件更新到最新版本，需要用户重新授予后台运行和无障碍功能权限”等，避免被网络犯罪分子诱导。

6、对已下载的可疑文件，可访问国家计算机病毒协同分析平台进行上传检测。

（央视新闻）

【反诈指南】

一不小心就中招，这四种常见诈骗套路一定要知道

元宵一过，新年已别。在大家投身忙碌工作的同时，诈骗分子也没闲着，快来 get 这份反诈指南，了解四种常见的诈骗套路，守护好自己的钱袋子吧！

警惕境外高薪招聘

境外直招　月入十万
包吃包住　朝九晚五
快醒醒！
这都是诈骗分子
精心设下的圈套

境外诈骗集团常以 “高薪工作、包吃包住、报销机票、专人接送”为诱饵，或以商务考察、免费旅游等名义将境内人员诱骗至境外，从事电信网络诈骗等违法犯罪活动。

警方提示：

请大家务必提高警惕，加强自身安全防范，找工作时要仔细甄别招聘信息，切勿相信所谓的“工资高门槛低”的境外招聘信息，避免陷入骗局和电诈陷阱。

机票“退改签”诈骗

冒充客服　航班延误
主动赔偿　屏幕共享
出行注意安全
更要提高警惕

诈骗分子通过非法渠道获取受害人订票信息后，冒充航空公司客服人员，通过打电话或发短信的方式，以飞机故障、恶劣天气等原因造成航班延误或取消，需要进行赔偿为由，要求受害人下载共享屏幕 APP，再引导填入银行卡号以及验证码等个人信息进行诈骗。

警方提示：

订购机票要通过官方途径、正规平台，避免信息泄露。当被告知航班延误或取消时，务必提高警惕，通过官方渠道核实信息真伪，退款一般都会原路返回。不要随意点击不明链接，也不要安装来历不明的 APP，更不要随意开启“屏幕共享”！

刷单返利诈骗

高薪兼职　轻松灵活
刷单点赞　垫付资金
天上不会掉馅饼
刷单肯定是陷阱

刷单返利类诈骗目前仍是变种最多、变化最快的一种诈骗类型，主要以招募兼职刷单、网络色情诱导刷单等复合型诈骗居多。诈骗分子初期通过小额返利骗取信任，后以“充值越多、返利越多”诱骗受害人做任务，再以“连单”“卡单”等借口诱骗受害人不断转账。

警方提示：

凡是打着“网络兼职”旗号，以返佣金为诱饵要求刷单、做任务、垫资的就是诈骗，不要相信低投入、高回报的说辞，切勿因小失大。

虚假网络游戏交易类诈骗

高价收购　免费赠送
转账交易　账户冻结
玩游戏可“别上头”
一不小心“跌跟头”

诈骗分子通过广撒网的形式，在游戏平台发布高价收购游戏装备、免费赠送游戏皮肤等虚假信息，与受害人建立联系后，诱导其绕过官方平台进行私下交易，或者要求添加“客服”进行交易。等到玩家付款后，以交易异常、操作失误为由，要求其缴纳手续费、服务费。

警方提示：

玩游戏时一定要保护好个人账号信息，不要向任何人透露自己的信息。游戏产品交易要通过正规或者官方平台进行，拒绝一切所谓“客服”的私下转账和交易。此外，各位家长也不要轻易向孩子透露支付密码。

（上海反诈中心）