以下消息描述了意大利的无政府主义同志如何被假冒成移动运营商技术人员的社交工程攻击所欺骗，从而在其手机上安装了间谍软件。

警惕镇压者通过诈骗在你的设备上安装间谍软件

来自意大利的教训

No Trace Project / 无痕，无案。这是一个工具合集，旨在帮助无政府主义者与其他反抗者了解敌人的能力，削弱其监控手段，并最终安全地采取行动，不被抓捕。

基于您的情况，持有某些文件可能被定为犯罪，或引起不必要的注意。请谨慎选择打印哪些小册子，以及将它们存放在哪里。

鉴于受害者的政治敏感身份及攻击者的技术能力，不难推测此次攻击的来源。因此我们敦促您警惕此类事件——尽管并非所有恶意软件都需用户主动安装（如本案所示），但防范意识仍不可或缺。

警惕镇压者通过诈骗在你的设备上安装间谍软件：来自意大利的教训

原文为意大利语

Potrebbe essere dannoso!

2025

brughiere.noblogs.org/post/2025/11/12/potrebbe-essere-dannoso

英语翻译

It Could Be Harmful! Spyware Installation Through Social Engineering Attacks in Italy

No Trace Project

简体中文（普通话）翻译

iYouPort

iyouport.notion.site/2e934ca2d46d80f8a3dbc5047b0ae709

排版

No Trace Project

notrace.how/resources/cmn-Hans/#lai-zi-yi-da-li-de-jiao-xun

这使得其即使未在屏幕上显示也能持续运行。

- 尤其是，授予了该应用所有权限，包括访问相机、麦克风、联系人、电话、短信、日历、位置、文件等等功能。
- 该应用的电池优化功能已在设置中禁用，因此其活动不会因节能而受限。
- 手机重启后，左上角立即出现绿色麦克风图标。随后该图标变为绿色圆点，最终消失。
- 更令人费解的是，此时居然还收到一条短信，询问："您对我的服务满意吗?"

经过此过程后，很可能所有手机数据（文件、媒体、联系人、消息等）均被此前通过欺骗手段安装的间谍软件应用转发到了远程服务器，使目标人的手机沦为了真正的窃听器——不仅能激活麦克风、摄像头和地理定位功能，还能截取屏幕截图。

无痕计划（No Trace Project）的注释：

以下消息描述了意大利的无政府主义同志如何被假冒成移动运营商技术人员的社交工程攻击所欺骗，从而在其手机上安装了间谍软件。根据我们的经验及其他同志的经历，我们认为文中所述的攻击：

- 极可能由国家行为体实施，可能是当地警方或检察机关。
- 极可能需要移动网络运营商的配合——他们会远程切断线路然后再接通，制造手机信号异常的假象，从而为假冒技术人员的干预提供可信度。

此事件应提醒我们：镇压当局的监控能力受限于其财政及其他资源。情报机构或许能获取更精密的间谍软件，实现更隐蔽更可靠的植入；而地方警察和检察机关则可能不得不依赖技术含量较低的手法。

这凸显了在运动内部普及社交工程攻击认知的重要性，以防其他队友落入此类陷阱。

我们近期观察到针对政界人士、企业、律师及活动家的间谍软件使用呈上升趋势。我们有理由相信，类似攻击正在被用于调查与反叛运动特定领域相关的个人。检察官或许更倾向于依赖外部初创企业提供的软件——尽管这些软件都不如 Pegasus、Predator、Graphite 或 Triangulation 等高端间谍工具精密昂贵，但仍能执行未经同意收集信息的告密功能。

近期部分同志遭遇移动设备入侵事件，过程是这样的：其手机突然无故失去网络及通话功能，所有外拨电话均被转接至运营商总机（或者受害者主动联系了运营商询问原因）。当在与一位工作人员通话后（此人要么表示不知情、要么不了解情况，并报告说可能是连接问题），随即有不同的号码来电，自称是运营商技术人员。

这个所谓的“技术人员”示意目标人的手机“尚未更新”。随后他会耐心细致地指导所有“恢复功能”的步骤，其中包括安

装一款带有 SIM 卡运营商名称和标识的应用程序。

安装步骤揭示了该应用的侵入性：

- 首先，禁用了 Play 商店中的 Play Protect 应用分析功能。该功能可保护设备免受潜在有害应用的侵害，确保已安装应用的安全可靠。
- 随后目标人收到一条短信，其中包含有指向该运营商官网仿冒页面的链接。页面引导用户点击酷似 Google Play 按钮的按钮下载“更新”。
- 文件绕过 Play 商店直接下载，用户需在忽略手机所有警告的情况下，从“下载”文件夹中打开该文件。为完成安装，必须修改手机设置允许安装此来源的应用。
- 之后，手机设置就被更改，允许访问移动网络，从而允许使用运营商的数据连接收发信息。
- 授予了该应用在后台运行的权限，并允许其在手机开机时自动启动。