M1+增效剂，我国科学家给抗癌病毒绑上“烈性炸药包”

治疗肝癌研究取得重要突破

中国科学家23日报告发现一种小分子化合物，能帮助抗癌病毒更有效地杀死肝癌细胞，其效果就好像给制导导弹绑上了“烈性炸药包”。这为治疗全球第二号癌症杀手——肝癌带来了新希望。

专杀癌细胞而对正常细胞无害的病毒被称为溶瘤病毒。世界上最早的溶瘤病毒报告出现在上世纪50年代，当时发现一名子宫颈癌患者在感染狂犬病毒后，肿瘤随之消退。2005年，我国批准将溶瘤病毒H101用于治疗难治性晚期鼻咽癌，这是世界上第一个由官方批准的溶瘤病毒药物。

中山大学颜光美教授团队23日在美国《科学转化医学》杂志上报告了在溶瘤病毒M1研究上取得的重要突破。M1病毒是1964年在海南蚊虫上发现的，它对人不致病，只在马和猪之间传播。2004年，研究人员在一次实验中偶然发现，M1病毒可将大鼠身上的胶质瘤溶解掉。

为提升M1病毒的抗肿瘤效果，颜光美团队在筛选了数百种临床抗肿瘤小分子化学药物后，发现一类小分子化合物能将M1病毒的抗肿瘤活性增强3600倍，而且对正常细胞没有毒性。

研究人员联合应用低剂量的M1病毒和这种增效剂，发现能将患人类肝癌的小鼠生存期延长一倍以上。在接近人类的食蟹猴上，M1病毒和增效剂的联合应用也表现安全。

颜光美对记者解释：“我们可以形象地将溶瘤病毒M1比喻为自动锁定肿瘤细胞的制导导弹，而增效剂的加入如同在导弹上绑定了自带筛选功能的烈性炸药包，强强联手，效果不言自明。将该方案应用于治疗在我国高发病率、高死亡率且缺乏有效药物的肝癌具有巨大潜力，给难治的肝癌带来了新的希望。”

（据新华社电）

延伸阅读 M1病毒曾被封存40年

1964年，一群科学家在海南岛“抓获”了50只蚊子，从这些蚊子体内，他们分离出了M1病毒。他们发现，M1病毒除了在马和猪身上会引起非常轻微的类似感冒的症状，对人和绝大多数动物都没有致病性。于是，这群科学家对M1病毒丧失了兴趣，病毒被封存。

2004年，正在写博士论文的胡骏在一次实验中偶然发现，M1病毒可以将大鼠的胶质瘤细胞溶解掉。

2009年，颜光美与胡骏发表论文，报告了他们在M1病毒身上的新发现——这种病毒在体外试验中能够杀灭癌细胞。

溶瘤病毒是一类具有复制能力的肿瘤杀伤型病毒，M1病毒也是其中之一。近几十年来，溶瘤病毒治疗引起了广泛关注，溶瘤病毒在美国得到大量研究，美国Amgen公司的溶瘤病毒免疫治疗药物T-Vec已经上市。

（据《南方都市报》）

江苏省消协发布手机APP侵犯个人信息安全警示

100多个手机APP，79个能定位、14个能监听

全民手机时代，消费者越来越离不开各种手机应用程序（下称“APP”）。然而安装APP时，常常被要求“读取通信录”“读取通话记录”“精准定位并获取行动轨迹”……不同意，担心被禁止安装或使用不畅；同意了，会不会泄露个人信息？江苏省消协8月23日发布的《关于手机应用程序侵犯消费者个人信息安全的新闻通报》揭露，大量APP未经用户许可就自动定位、读取通信录、发送短信等，甚至还能监听电话！

100多个APP中 79个要求获取定位权限

下载一款APP，到底会获取多少你的个人信息？江苏省消协法援部工作人员傅铮用自己的小米手机，向记者进行了展示。

下载软件“爱奇艺”，安装时，打开“权限设置”发现，“定位、获取手机信息、访问日历、访问相机、录音、读写手机内存、读写系统设置、后台弹出界面”这8项内容已经被默认勾选“允许”，如果消费者不注意，软件安装时将自动获取这些权限。其中只有“桌面快捷方式、锁屏显示”这两项内容，在安装时被默认“拒绝”了。而“发送短信、直接拨打电话、监听电话、读取联系人、访问手机账户、开启WiFi”这6项内容处于“询问”状态。

不仅是这一款软件，通过现场检测，该手机共安装了100多个APP，其中79个APP可获取定位权限，91个APP可以获取手机信息。而“短信和彩信”这一项上，有23个APP获得权限后可以直接向通信录上的联系人发送短信，有96个APP可以直接发送彩信。

让人大吃一惊的是，点开“电话与联系人”一项，竟然有14个APP可以监听电话和挂断电话。

常收到广告 可能是因为给了APP这个权限

这些APP为什么要获取这些权限？记者了解到，在APP要求获得的所有权限中，“位置信息”和“读取通信录和软件”是最普遍的。如果你用的是苹果手机，打开设置里的“隐私”，也能看到要求使用“定位服务”和访问“通信录”的所有应用。

“大多数APP都要求使用GPS定位，而且是精确定位，可精确到10米。APP开发企业给出的理由是社交模块需要这项功能。”江苏致邦律师事务所律师陶若晨介绍，比如，一款阅读软件开发企业表示，定位后用户可以看到周围的人在读什么书。“但我们认为，想要实现这个功能，获取大致位置权限就可以了，不需要GPS精确定位”。

对于获取“读取通信录和短信”权限，陶若晨表示，大部分APP开发企业给出的解释是需要短信验证码，避免重复注册。很多人会收到广告推销短信或者电话，你的电话号码很有可能就是这些APP泄露的。“比如，你的朋友使用了某款APP，APP获取了读取通信录的权限。如果你的号码在他的通信录上，APP就会自动给你发短信。”陶若晨说。

而一旦被APP开发企业获取了这些信息，用户的生活和隐私就完全透明了。“你每天给什么人打了电话，你每天的行动轨迹、上下班时间，他们都能知道，你的生活完全被别人监控了，想想就感到非常恐怖。”江苏省消协投诉部主任张昊舒表示，这些个人信息一旦被泄露、丢失，带来的风险是各种各样的，完全没法儿预估。

视频、购物类APP为啥要监听电话

APP竟然能“监听电话”，这就更加让人难以理解了。

记者了解到，需要获取这项权限的APP种类五花八门，有理财类、视频类、购物类等。这些APP为什么要监听用户的电话呢？

“这其实也是我们非常困惑的问题，我们也在向开发企业提出疑问，希望他们予以说明。”张昊舒告诉记者，其中一家APP开发企业的回应是，监听电话是为了防止有人以该软件的名义拨打诈骗电话。“这个理由我们觉得是站不住脚的，不是正当合法理由”。

张昊舒表示，大部分APP申请的大量手机权限，远远超出了手机APP正常为消费者服务所必须获取的权限，属于过度收集消费者个人信息。

默认授权和过度授权让用户成“透明人”

让人觉得可怕的是，很多权限被APP获取是在不知不觉中完成的。

“我们现在能看到的这些权限设置，并不是全部的，只是我这个手机能检测出来的。还有很多品牌的手机，消费者完全看不到权限设置，软件就已经自动安装完毕了。”张昊舒介绍，绝大多数APP下载安装完成前均未向用户提供选择授权的机会，也没有明确告知用户获取权限后收集、使用个人信息的目的、方式、范围和风险。只有极少数品牌的部分机型会在APP安装完成前明确提示。还有部分机型存在默认开通所有权限的情况。

经调查，只有部分操作系统为安卓6.0以上版本的手机，会在用户使用APP过程中对少数权限进行触发提示选择，大多数品牌和型号的手机需要消费者自行进入手机设置中进行手动选择，且没有任何提示或说明。

江苏省消协的调查发现，同款APP，安卓版本的权限获取需求远远大于苹果版本。

陶若晨介绍，个人信息包括姓名、身份证件号码、联系方式、住址、账号密码、财产状况、行踪轨迹等。按照《消费者权益保护法》和《网络安全法》，经营者收集使用消费者个人信息应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。同时，还要对信息进行保密。

“获取定位”“读取通信录”等已经涉及个人隐私。“过度收集个人信息显然已经超出了合理正当的范围，而且APP开发企业没能建立比较完善的个人信息保护规则和措施。”陶若晨表示。

取消授权并不影响大多数APP正常使用

对于用户来说，怎样才能躲过APP的重重陷阱，保护自己的隐私？还有用户担心：取消了授权，APP是不是就用不了了？

记者进行了试验，将某视频APP的所有权限全部关闭，再重新打开该APP，随机点开一个视频，完全可以正常播放，没有任何影响。“很多APP其实不需要那么多权限，如果关闭授权影响了必要功能的使用，APP会提醒你。”傅铮介绍。

对此，江苏省消协提醒消费者，一方面，可以通过手机系统设置或者第三方检测软件，查看、修改APP的授权情况，把不必要的授权取消；另一方面，在下载新的APP时，要到正规APP商店下载。下载安装APP时，注意查看权限设置，把所有不影响正常使用的授权全部关闭。

（据《现代快报》）