谨防“超级病毒”感染手机

日前，一种被称为“超级手机病毒”的恶意软件大爆发，因其会群发短信给通讯录好友，传播范围十分广泛，引起公众极大恐慌和关注。如今，手机几乎成了很多人的一个“器官”，可一旦这个“器官”被病毒攻击该怎么办？

“为了好玩”，湖南小伙制造“超级手机病毒”

8月2日凌晨1时许，深圳警方陆续收到受害群众报案称：手机收到短信：“×××请看http://……”，点击该短信内的链接后，会下载一种叫“××神器”的软件，该软件自动盗取其手机通讯录、手机短信，并且会再次群发短信给通讯录联系人。

“××神器”木马病毒危害极大，迅速在全国范围内形成爆炸式传播，并被冠以“超级手机病毒”的称号，造成了较大影响。

据警方通报，8月2日18时许，在深圳市宝安区龙环一路某小区将涉嫌制作、传播“××神器”手机恶意程序的犯罪嫌疑人李某成功抓获，并查清该恶意程序根源。

8月3日，深圳市公安局召开新闻发布会称，病毒制造者是中南大学19岁大一学生李某，湖南邵阳人，来深圳过暑假。李某对制作传播该恶意程序并非法获取公民个人信息的行为供认不讳。据李某供述，制作此款恶意程序的动机就是“为了好玩”、“想做一款能够大范围传播的软件以证明自己”。

警方通过对嫌疑人后台查找，发现了大量用户的银行、支付宝等动态密码，资金余额等涉及财产的短信。据警方透露，由于侦破及时，尚未发现嫌疑人非法获取的公民个人信息被用于非法用途。

手机短信病毒危害大

1、可“吸”短信费

不少受害者表示，接到朋友类似短信，没想太多就点击了链接，就发现自己的手机在自动发送短信，一天发送的短信费可能超100元。

2、可窃取用户隐私

360手机安全专家分析发现，该病毒一旦被打开运行，会要求用户填写用户名、密码、姓名及身份证号等隐私信息，提交后会发到一个指定的手机号码上，因此可以轻易盗取用户隐私信息。

3、人际传播传染性超强

金山毒霸信息安全专家李铁军表示，从病毒特征分析看，该病毒类似此前的蠕虫病毒，其危害较大。由于该病毒是通过通讯录中的名单传播，导致其在很短的时间内大量感染手机。

三大运营商：拦截千万条短信阻断病毒

中国电信、中国移动、中国联通针对8月2日爆发的恶意手机病毒“××神器”，在第一时间采取多项应急处理措施，在全国范围成功拦截该病毒短信千万余条，并阻断病毒下载链接。目前，该恶意手机病毒的扩散已得到有效控制。

专家提示，已受感染用户可通过依次点击手机“设置——应用程序——应用程序管理”，选中“com.android.Trogoogle”和“××神器”，选择“卸载”，点击“是”来卸载该组恶意应用程序。

国家计算机病毒应急处理中心建议：

1、通过恢复手机出厂设置来彻底根除病毒。

2、用户如果怀疑可能已经被感染，应马上停止网络连接，与运营商联系，核对通信话单，检查短信记录和网络使用记录，发现来源不明的短信发送行为和网络访问请求，并立即更改手机应用的账户密码等隐私信息，尤其是金融支付类、通信类相关的应用，以免造成进一步损失。同时告知通信录中的亲友，请勿轻信可能由本机号码发出各种虚假信息。

3、目前，360、恒安嘉新、安天、瑞星、金山、趋势科技这几家公司的防病毒产品可以进行防护。

（本报综合）

凤眼时评 >>

超级病毒吸话费，手机安全应立法

文／龙敏飞

超级手机病毒七夕作案，其声势之大令人惊讶，其传播之广令人害怕。这意味着，不仅在互联网时代，而且在智能手机时代，我们的信息安全同样处于“裸奔”的状态。然而，随着社会的发展与进步，智能手机、互联网已经与我们的生活融为一体，不可分割。在这样的境况下，确保手机安全，无疑是迫在眉睫的。

对于当前这起超级病毒案件，很多人认为，虽然每个人的损失不多，但肯定不能让用户当冤大头。一则，犯罪嫌疑人已经抓获，理应对其进行一定的经济处罚，而这些处罚款理应返还给用户；二则，即便是犯罪嫌疑人作案，运营商其实也是获利者，因为其收到了一定的短信费，这笔钱是否“取之有道”，仍是存疑的。简言之，在公众的认知下，无论是犯罪嫌疑人还是运营商，都应为超级手机病毒承担一定的责任。

遗憾的是，记者咨询了三大运营商的客服人员，均称对于已损失的话费，无法直接返还。而律师也坦言，类似的民事诉讼由于事主很难获取证据，因此即使起诉，也很难达到预期的诉讼结果。也就是说，对于手机安全，运营商是靠不住的，维权渠道是走不通的，关键还得靠用户炼就一双“火眼金睛”。

如果说，这仅是个案，那也就罢了，权当“花钱买经验”，但很显然，这并非个案——2013年11月，浙江嘉兴的汪女士因为误扫恶意二维码，导致手机被植入短信劫持木马，最终导致被盗刷18万元；今年1月，著名影星汤唯被电信诈骗21万，而剧组所有人都同时收到了诈骗短信等等。此外，根据统计，2013年受恶意吸费应用感染用户人数高达1400万，致使用户直接经济损失超过7000万元。在这样的现实氛围里，对于超级病毒事件，的确需要认真审视。

调查数据显示，2013年我国智能终端出货量达2.24亿部，成为全球最大的智能手机生产国，这就是说，智能手机的安全，与很多人的生活息息相关。在这样的现实语境里，手机安全的确不能再处于监管的真空地带。对此，全国人大代表徐龙就曾建议：“目前国内仍没有明确的关于手机安全的法律法规，对制造和传播手机病毒的单位个人没有明确的惩罚规定。这需要国家尽快立法，保护公众手机通信安全。”这样的建议，既是对民意的一种呼应，也是应对信息化时代的必须之举。

因而，超级病毒吸话费，手机安全当立法。唯有软件应用商场安全标准和手机应用安全标准有据可依，安全立法也照进现实，再面对手机病毒吸话费的案例时，其背后的责任划分才能厘清，监管者才不至于束手无策，用户也不会是冤大头。也唯有如此，才能更好地维护手机安全。