

警告 勒索软件已在安卓手机上出现！！

防范手机应用的重要性！



嗨~大家好！
我是小信！很高兴认识大家！

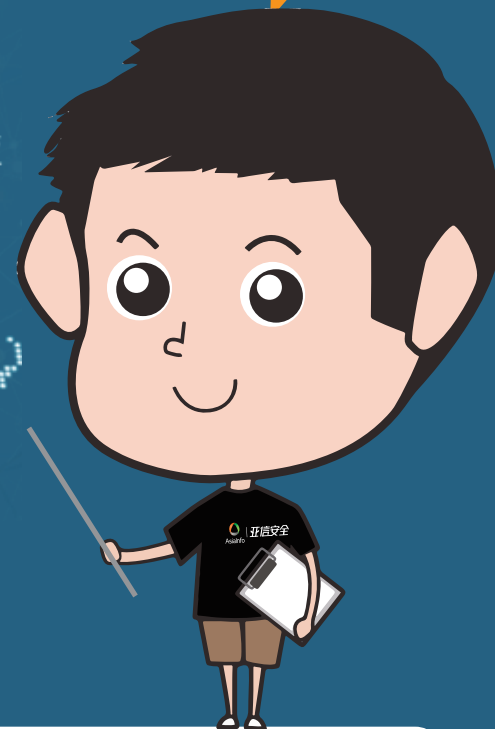


嗨~大家好！我是小亚！以后就由我和我的小伙伴--聪明美丽的小信一起为大家讲解关于亚信安全的案例。

Android移动端平台群众基础巨大，正逐步受到网络犯罪的侵袭~手机安全不可小觑啊!



嗨~大家好!今天由我和小信一起为大家带来最前沿的安全资讯~这都是亚信公司的独家报道哦~

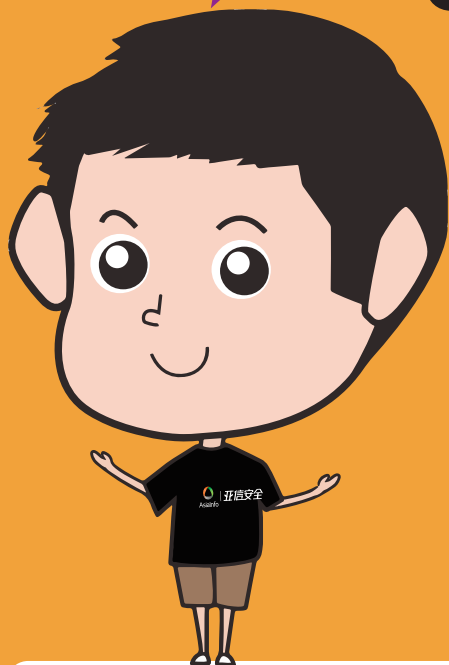


勒索病毒如同瘟疫一样疯狂的向全球蔓延，仅18个月时间，勒索病毒就占据了安全领域的大部分版图，不论是数量还是破坏力都达到了惊人程度。亚信安全研究院调查显示，2016年6月Android勒索病毒威胁比2015年4月增长了15倍!网络犯罪集团现在已把矛头指向另一目标：Android移动端平台。

一旦遇到这种情况，只有交赎金了？难道我们就只能被犯罪分子牵着鼻子走？



要防范这样的情况发生，首先我们要时刻注意自己日常使用手机的习惯~

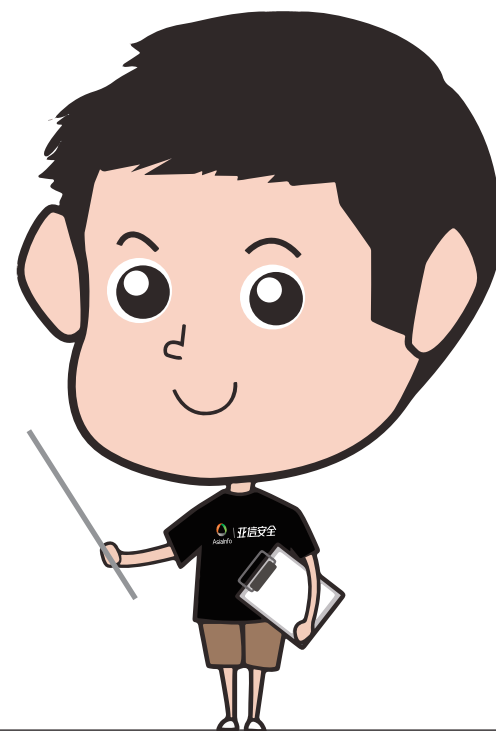


移动设备勒索病毒如何威胁受害用户？

勒索病毒的可怕之处在于，不管你的台式机还是移动设备只要被它锁住或加密文档，那么你只有向黑客支付赎金的份儿。如果你不照做，犯罪者会将你被感染的文档、照片或视频文件统统删除，严重情况会让你永远无法使用电脑或移动设备。亚信安全研究院在2014年4月首次发现了移动勒索病毒的样本，这种病毒变种体以锁住手机屏幕的方式要挟用户支付赎金，一旦受害者拒不支付，它将完全控制移动设备的执行指令，直接迫使用户购买新的手机。有时它也会冒充监督部门或执法机关，在手机屏幕上显示调查令来逼迫用户缴付“罚款”，总之，越能装饰自身强势身份，黑客就越是乐此不疲，而最终被恐吓勒索的则是那些受骗的用户。



APP也有山寨李鬼！
平时使用APP时，要
从正规安全的商店下
载，轻易不要点击未
知链接或应用程序。



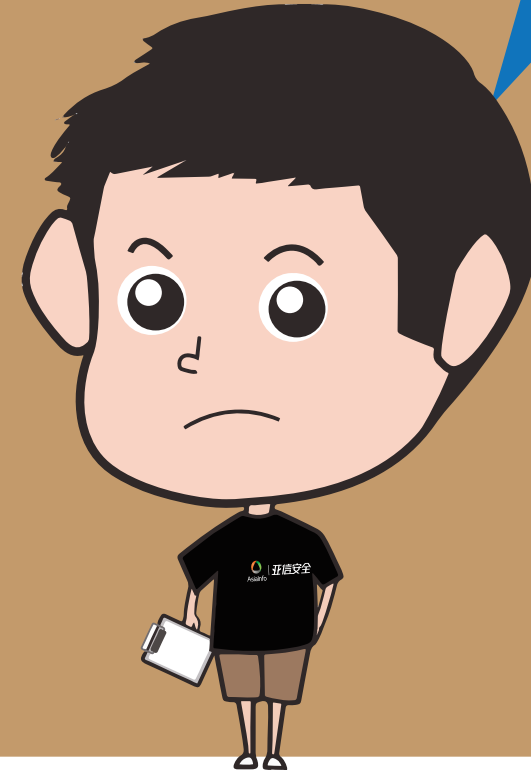
移动设备勒索病毒的扩散根源在哪里？

通常情况下，移动勒索病毒喜欢冒充常用的应用程序、热门游戏、Flash播放程序、视频教程、系统更新程序加载到用户系统里，他们大多来自非官方的APP下载资源中。此外，用手机登陆网站论坛、浏览情色网站或是点击简讯中的垃圾链接都有可能遭到勒索病毒的攻击。



俗话说，好奇害死猫~所以大家平时要尽量控制不安的好奇心，注意来路不明的APP ~

总之~最安全的办法就是安心工作，多做户外运动，少做低头族就好啦啊~



移动设备勒索病毒威胁不断加大，如何有效进行防范？

首先，就像上面提到的情形，不在那些非法的APP平台下载软件，浏览网站时尽量控制自己的好奇心，不点击未知页面或链接，以免涉入感染源。