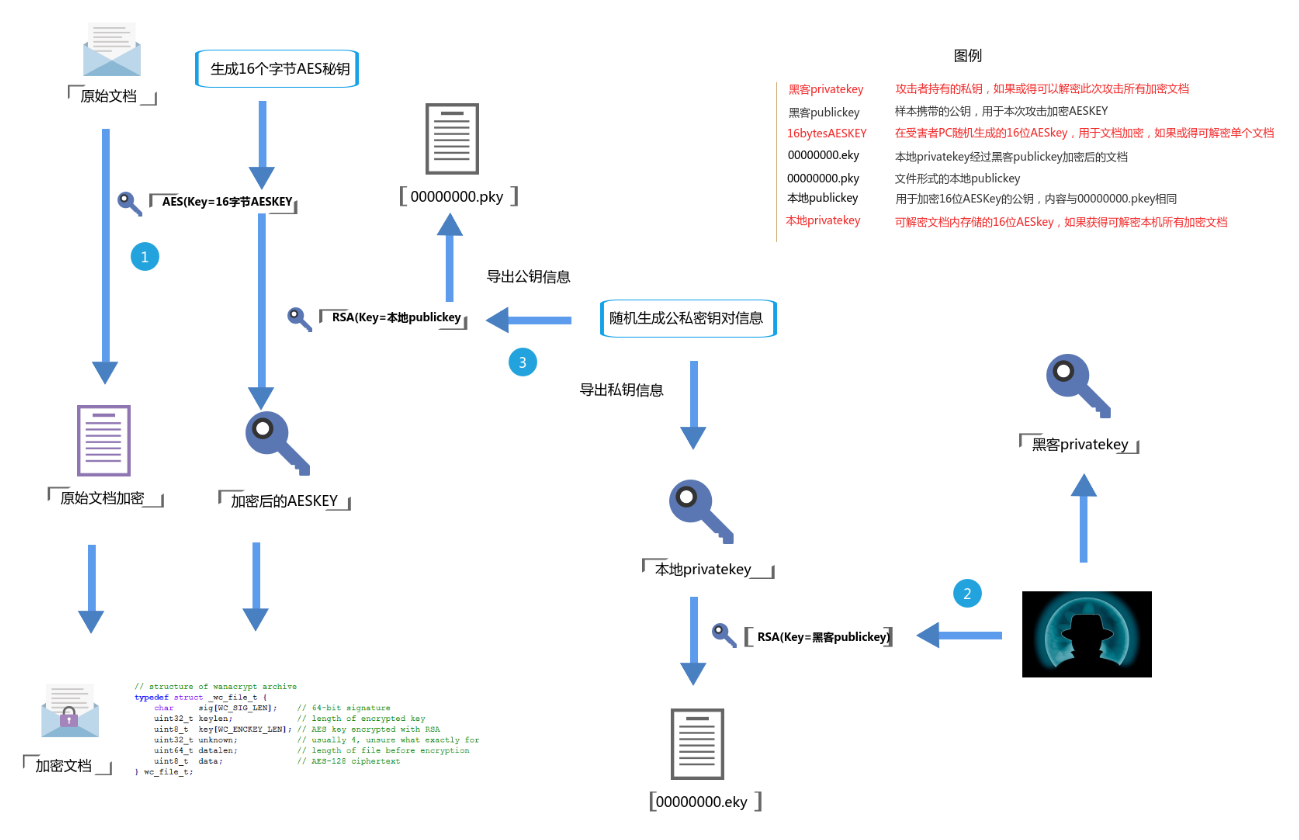
**一张图看懂WannaCry的套路之深**

最近几天，全球爆发大规模WannaCry勒索病毒攻击，对windows系统用户造成了较大影响。下面我们就带您一起了解下WannaCry病毒使用的五个套路，感受该病毒的狡猾之处。

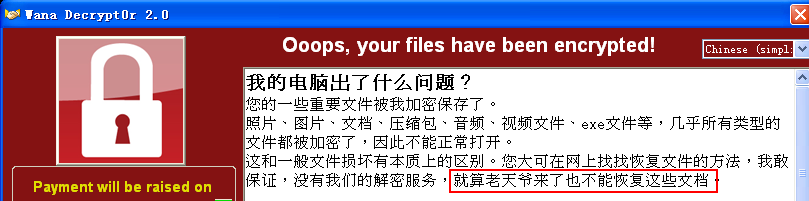
**套路一：眼花缭乱的加密流程**

先看下WannaCry整体的加密流程：



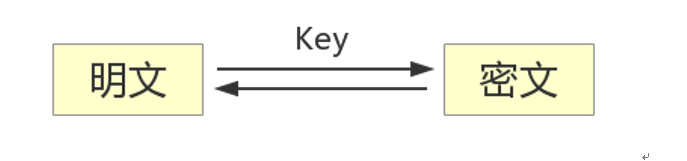
1. 病毒随机生成16个字节的AES Key，对文件内容加密。
2. 黑客手里握有一对公私钥，把公钥放在病毒体内传播，私钥自己保管。
3. 病毒自动随机生成一对公私钥，私钥用病毒体内的公钥加密后保存,公钥用于对AES Key加密，然后保存在加密后的文件内。

**套路二: 老天爷也无法解密的加密算法**



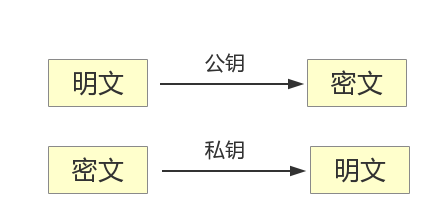
病毒为什么会夸下如此海口，号称老天爷来了也无法恢复文档？这要从病毒所使用的加密算法说起。病毒对文件加密采用的是RSA算法，RSA算法是一种非对称加密算法，与之相对的是对称加密算法。两种算法的应用的场景有所不同。

我们先简单说下对称加密算法，对称加密算法只有一个key，加解密都使用同一个key，比如我们可以通过key把A加密成B，同样使用该key可以把B解密成A。



所以如果病毒使用对称加密算法来加密文件，在病毒加密的时候我们就能知道用于加密的key了，同样使用该key就可以解密文件了。因此敲诈勒索病毒一般不使用对称加密算法。

而非对称加密有所不同，非对称加密有两个key，分别称为公钥和私钥，公钥用于加密，私钥用于解密。比如我们通过公钥把A加密成B，必须使用私钥才能把B还原成A。

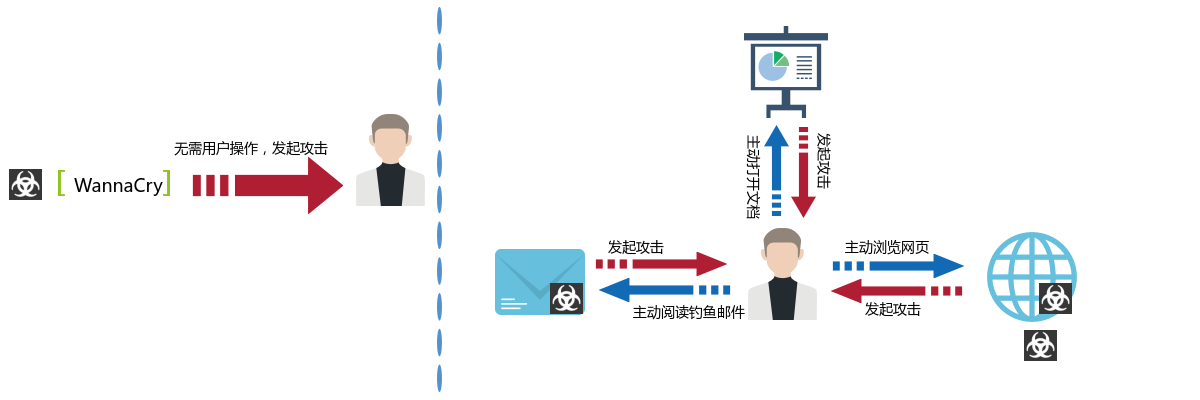


虽然非对称加密区分公私钥，安全性较高，但相比对称加密速度较慢，不适合对大量数据加密。所以一般与对称加密结合使用，用非对称加密的公钥去加密对称加密的密钥，保证对称加密密钥的安全性。

因此WannaCry同时使用对称加密算法（AES）与非对称加密算法（RSA）。先用AES加密来加密用户文件，然后又使用RSA公钥加密来加密AES的密钥，而私钥只有黑客自己知道，所以在没有黑客手中私钥的情况下，很难解密文件。

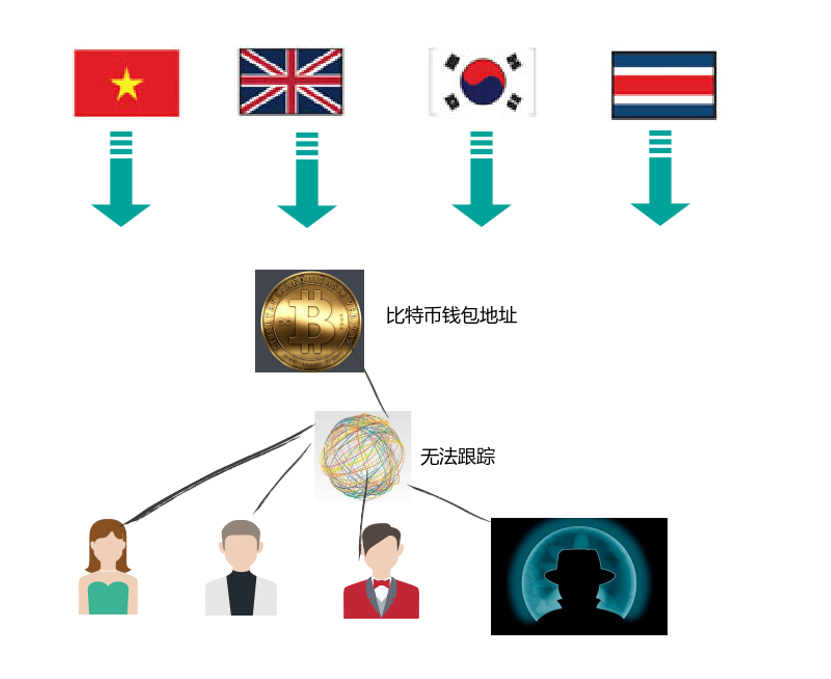
**套路三: 主动出击的传播方式**

一般病毒的传播方法包括浏览器漏洞传播，office文档传播，邮件传播等。但WannaCry所使用的是Windows远程漏洞传播，也就是说用户只要开着电脑，不用做任何操作，就有可能遭到攻击。



**套路四: 狡猾的比特币支付**

比特币是一种虚拟的数字货币，黑客只需要提供一个自己的比特币钱包地址，然后其他人就可以通过该地址向黑客转入比特币了，并且根据该地址无法追踪到黑客本人。其次比特币不受地域性限制，全球的受害者都可以付款。



**套路五： 你以为给钱就行了？**

在比特币交易和银行转账不同，在比特币交易中，收款人无法确认付款人信息。黑客只能通过付款人使用的钱包地址区分付款人信息。所以以往的敲诈病毒都通过对每一个感染的用户机器上生成不同的钱包地址让用户支付比特币。而这次WannaCry敲诈者只使用了三个比特币钱包地址，每个用户的赎金地址都是从这三个钱包地址随机选一个。所以黑客只能看到自己的比特币钱包里的钱在涨涨涨，但不知道究竟是谁向他转的钱，也就无法知道该对谁进行解密服务。可见套路之深，黑客根本不关心是谁中了毒，谁的文件被加了密，只关心自己的钱包，又或许黑客一开始就没打算给用户解密。  
