对于一个技术高超的攻击者来说，肉鸡获取的手法有多种多样。但是，与所有人一样，攻击者也喜欢那些即简单又容易获取肉鸡的方法。就目前来说，利用特洛伊木马和社会工程学就是攻击者们最喜欢用来获取肉鸡的主要方式。   
　　1、 利用捆绑木马和网页木马来获取肉鸡  
  
　　木马，就如同一个身怀多种绝技的“武林高手”，在网络的江湖之中，将所有坏事做尽，却仍然没有人可以阻止它继续前进的脚步。因此，木马是许多网络攻击者们最喜欢使用的“干将”。这不，对于肉鸡猎手，木马就如同他们带着的猎犬，能够嗅到最敏感的东西，能通过木马得到他们想要的“肉鸡”。  
  
　　当然，就木马本身而言，其技术有好有差。而且，木马技术并不是一成不变的，它会长江后浪推前浪，不断地向更高级、高隐蔽、更高性能的方向发展。  
  
　　同时，木马的数量也在不断地增加。就拿能够获取肉鸡的木马来说，现在，在GOOGLE文本框中输入“肉鸡获取软件”的关键词进行探索，一不小心就会得到N多获取肉鸡木马的软件说明或下载链接。雪源梅香就曾经试过两个叫肉鸡批量抓取和挖掘鸡的软件，这些软件名字取得很形像，功能也相当不错，能够让一个不了解多少网络知识的人轻易地获取大量的肉鸡，更不要说网上还有许多获取肉鸡的“指导手册”和“指导视频”呢。  
  
　　从这可以想像木马拥有多么可怕的“功夫”。那么，这些木马主要又是通过什么方式去获取肉鸡的呢?  
  
　　主要方式有两种：  
  
　　(1)、一种是利用各种捆绑方式  
  
　　木马捆绑一直是攻击者最常用的散发木马的主要方式之一。可以用来捆绑木马的载体包括垃圾邮件的附件、软件安装程序、自解压压缩文件、PDF文件、MP3、MP4，以及图片等等。  
  
　　这种木马攻击方式，就是先将木马通过捆绑的方式加入到上述这些载体中，然后放到互联网上，成功引诱网络用户运行这些载体中的木马程序后，这台主机就有可能会变成攻击者的肉鸡了。  
  
　　通过捆绑木马方式获取肉鸡，要成功的关键就是想法让网络用户运行被捆绑载体中的木马。攻击者最喜欢使用的手段包括将木马与黄色图片或视频捆绑，与免费软件捆绑，与MP3及PDF文件捆绑，然后将捆绑了木马各种文件放到一些正常网站或自己建立的傀儡网站上，提供给用户下载或试听等。攻击者还会通过QQ、MSN等即时通信软件，主动发送捆绑有木马的图片、视频和文件给用户去打开执行。或者通过即时聊天软件发送中奖等信息，引诱用户运行载体中的木马。由于这些手段有很高的欺骗性，致使许多网络用户上当受骗。  
  
　　(2)、另一种就是通过网页挂马的方式  
  
　　攻击者另一种最喜欢用的方式就是通过网页挂马了。这种方式主要是通过将木马程序挂载或嵌入到正规网站或自己建立的网站中，当用户进入这些网站进行浏览时，就会自动执行木马激活脚本，从而让用户主机变成攻击者的肉鸡。  
  
　　现在，还有一种高超的木马攻击技术，就是将木马嵌入到QQ的聊天信息当中，而且只需要用户查看QQ即时信息就可以激活其中嵌入的木马。  
  
　　网页挂马的方式比第一种方式更容易让用户中招，主要是这种方式更加隐秘。攻击者也更加喜欢将木马挂载或嵌入到一些知名的大型网站当中。这是由于许多用户都相信这些网站，并且这些网站每天在线的用户数量又多，因此，当这些大型网站上某些网页被挂载或嵌入木马后，就会让大量用户在毫不知情的情况感染木马而轮为肉鸡。  
  
　　从上述两点不难发现，使用木马方式获取肉鸡，一旦网络用户执行或打开了捆绑了木马的文件，或者浏览了挂载了木马的网站，由于现在的木马大多都具有很强的免杀能力，用户系统中的杀毒软件或防火墙有可能对这些木马无能为力，用户主机也就这样轻而易举地成了黑客的肉鸡。  
  
　　虽然使用这种方式能够大大提高黑客获取肉鸡的速度和成功率，但是，一些以技术为主的黑客是不愿意使用这种方式来获取肉鸡的。反而，一些没有什么网络技术和编程能力的攻击者，就喜欢使用这种简单容易的方式来获取肉鸡。  
  
　　只是，真正意义上的黑客人数要比这类攻击者少很多，因此，如今互联网上绝大部分的攻击都是通过利用木马来进行的。这也是为什么互联网中到处埋有木马，让所有的网络用户不敢轻易踏入“雷池”的主要原因。  
  
　　2、 利用社会工程来获取肉鸡  
  
　　对于一些攻击者来说，他们非常乐意使用社会工程学原理来获取肉鸡。通过这种方式，获取肉鸡，有时只需要打一个电话这么简单。  
  
　　例如，一个攻击者使用一台公用电话或其它用户不熟习的号码，冒充电信公司某个新来的客户代表打电话给用户，告诉用户由于电信公司的网络系统正在升级，现在需要用户提供其主机的登录帐户和密码，用来将用户信息输入到电信公司的新系统中，以便用户网络也随同一起自动升级。对于这样的电话，有很多网络用户会不加怀疑就轻易地相信，一旦我们将这些信息如实告诉他，那么，我们的主机就如同一栋没有锁门的房子，这位攻击者想进就能进了。  
  
　　其实，只要我们稍微多想想，这样的电话就漏洞百出，因为不管电信机房网络系统如何升级，也不关用户主机登录帐户和密码的事。  
  
　　还有些攻击者更喜欢直接接触用户的方式来控制用户的主机成为肉鸡。例如，他们会冒充计算机销售商的客服人员，穿上一套与这个计算机销售商相同或相似的工作服，带上假的或盗取来的工作牌，来到用户家中，告诉用户他们是来进行定期上门维护的，并告诉用户由于某种活动增加了上门服务的次数，一般的用户对于这些多出来的免费上门维护是不会拒绝的。然后，他们就会要求用户提供主机的登录帐户和密码，以便他们能进入系统进行检查，此时，一些用户仍然会马上将这些重要信息告诉他们，就这样，黑客在得到了用户的帐户和密码后，进入系统并趁机安装上后门程序，然后潇洒地离开，而用户的主机就这样成为了他们的肉鸡。  
  
　　大家可能认为这些社会工程学方式每次只能得到一台肉鸡，那就是你不知道怎么做而已。如果攻击者到一家具有长话联盟的宾馆开一间房，他就可以使用宾馆提供的免费电话来得到数量众多的肉鸡，甚至可以通过这种方式得到某个企业整个内部局域网中的所有主机。  
  
　　同时，攻击者还可以将社会工程学与其它两种获取肉鸡的手段进行结合使用，来加快获取肉鸡的速度和提高成功率。例如，攻击得可以先通过社会工程学方式来获得目标的IP地址、使用的操作系统等信息，然后通过弱点扫描工具对这些目标主机进行扫描，再植入木马至目标主机;或者通过社会工程学方式去引诱用户直接运行捆绑有木马的各种文件等等。  
  
　　实际上，攻击者除了利用系统漏洞、木马和社会工程这些主要的手段来获取肉鸡以外，他们还在不断地开发新的方法，例如自己编写批量抓鸡工具，利用不设防的无线网络等。因此，我们在了解这些常用手段的同时，还应当关注各种新出现的攻击手段和技术，以便能及时了解这些新攻击手段和技术的攻击原理，并及时掌握相应的防范措施来应对它们