社会工程学攻击简析

王艳阁，高 丽

（中原工学院信息商务学院，河南 郑州 450000）

摘 要：随着网络社会的发展，人类的生产生活越来越依赖于网络，习惯于通过网络来传递信息，这就在传统的网络安全基础上，给个人和组织带来了更大的挑战。社会工程学攻击是一种针对人或者人性的攻击手段，它比传统的攻击方法的目的性更明确，手段更具欺骗和隐蔽性，因此每个人在加强自身安全意识的同时，结合更先进更智能的检测手段和安全设备，才能更加有效地对社会工程学攻击进行防范，减少或避免损失。

关键词：网络安全；社会工程学攻击；防范

在当今这个高度信息化的社会，黑客们如何通过邮件、IM、社交网络等渠道，对组织或企业实施有针对性的先进攻击，以获取组织和企业内部的相关的保密信息，并最终盗取企业或组织的核心信息或对其关键业务进行攻击。

近年来，爆出的重大APT攻击者，无论是针对Google等三十多个高科技公司的极光攻击，还是针对RSA窃取SECURID令牌种子的攻击，甚至到针对伊朗核电站的震网攻击，都能看到社会工程学攻击在整个APT攻击中所起到的至关重要的作用。

社会工程学是一种通过受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段，它并不等同于一般的欺骗手法。可以说社会工程学攻击和网络渗透攻击的目的都是一样的，都是为了获取自己想得到的东西，但是两者的攻击目标不一样，最大的区别是渗透攻击的目标是机器，而社会工程学攻击的目标是人，那些有思想有欲望的人类。

下面针对APT攻击案例分析，Google等三十多个高科技公司的极光攻击：攻击者通过FACEBOOK上的好友分析锁定了Google公司的一个员工和他的一个喜欢摄影的电脑小白好友。攻击者入侵并控制了电脑小白好友的机器，然后伪造了一个照片服务器，上面放置了IE的0DAY攻击代码，以电脑小白的身份给Google员工发送IM消息，邀请他来看最新的照片，其实URL指向了这个IE 0day的页面。Google的员工相信之后打开了这个页面然后中招，攻击者利用Google这个员工的身份在其内部持续渗透，直到获得了Gmail系统中很多敏感用户的访问权限。窃取了Gmail系统中的敏感信息后，攻击者通过合法加密信道将数据传出。在案例中，起到先锋至关重要的都是社会工程学攻击。

通过案例可知，在进行APT攻击的最初阶段，攻击者都通过各种手段收集信息，和攻击者进行内容的交互，成功欺骗了被攻击者后，通过一个小小的跳板，最终获取到所需要的信息，这就是社会工程学攻击。

社会工程学的具体内容和攻击步骤如下：

首先，社会工程学攻击者都是一个优秀的信息搜索专家，通过各种搜索引擎、社交网络、IM甚至包括电话来获取到想要的一切信息。攻击者可以通过搜索引擎，结合高级搜索应用技术，在浩瀚无垠的网络世界中，获取到被攻击的组织或个人有意或无意间留下的各种痕迹，从而分析出组织的组织结构、人员基本信息等，为进一步通过电话或网络实施欺骗打下基础。

当攻击者收集到了足够的信息及分析后，就会继续下一步的行动——欺骗。攻击者通过伪造身份证、伪造经历以及编纂故事等手段，通过社交网络、论坛、邮件、即时通信软件或电话等途径，与目标建立联系，并通过沟通逐渐获取目标的信任。攻击者可能伪装成目标的好友，也可能伪装成一个有问题需要咨询的客户，和可能伪装成相关业务部门的同事，甚至是伪装成目标的上级，极端的个案中，攻击者甚至伪装成对公司业务有兴趣的投资人从而获取相关信息。当目标接受了攻击者的伪装身份后，自然而然地产生了对这个身份的信任和盲区，从而给攻击者实施攻击提供了可能。

最终，攻击者通过获取到的信任感以及收集到的其他信息，通过木马注入、Oday攻击、钓鱼网站等一系列最终技术手段，实施攻击并获取到相关信息或为下一步的深入埋下一颗颗钉子。

通过分析可知，社会工程学攻击实际上是通过信息收集、活动交互、欺骗等手段，最终达到目标人物实施攻击的一种手段。但目前无论是个人还是组织，对于信息安全的建设及装备投入都已经非常重视，一个组织可能购买最知名的防火墙、最强大的IDS或IPS系统，从安保公司雇佣了最好的保安，使用了最先进的反病毒软件以及补齐了操作系统的所有已知漏洞，但是，我们仍然不能保证你的信息不被泄露出去，因为，是人就会有弱点，而社会工程学攻击恰恰是针对于“人”的攻击。

应该如何防范社会工程学攻击呢？本文从以下两方面做出总结：

首先是个人信息的安全保证：当前各种网络服务及应用的普及，每个人都是自己生活的直播者，如何在满足个人信息发布需求同时，更好保护自身的隐私是每个人都需要考虑的事情，是对社会工程学攻击防范的第一步。

其次，组织在网络安全建设和规章制度的制定上，需要更多地考虑执行，再好的防范措施和制度，如果没有一个有力的执行，也都是空谈。

社会工程学攻击是一种针对人或者人性的攻击手段，它比传统的攻击方法的目的性更明确，手段更具欺骗和隐蔽性，因此只有在每个人都加强自身安全意识的同时，结合更先进更智能的检测手段和安全设备，才能更加有效地对社会工程学攻击进行防范，减少或避免损失。

参考文献：

[1]靳慧云；黑客入侵技术和方式变异论析[J]；中国人民公安大学学报(自然科学版)；2007年04期.

[2]罗亚萍；社会政策目标选择对就业政策的影响[J]；西安交通大学学报(社会科学版)；2009年01期.