利用传染性媒体生成器入侵计算机

黄长江[1] 詹柳春[2]
（1.广州大学松田学院 广州 增城 511370;
2.广东工业大学华立学院 广东 广州 511325）

[摘 要] 随着计算机水平的发展，我国面临严峻的网络安全问题，恶意代码数量呈现几何级数增长态势，严重危害着现代网络的安全运行，而作为恶意代码家族中一个重要成员的木马，其破坏能力不容小视。本文通过一个较为完整社会工程学实例“传染性媒体生成器”来展示入侵过程，以此呼吁广大计算机用户提高网络安全意识。

[关键词] 媒体生成器；社会工程学；恶意代码

1 概述

本文首先介绍与传染性媒体生成器有关的一些概念，再通过一个较为完整的社会工程学实例“传染性媒体生成器”来展示入侵过程。另外，本文实验环境真实，所涉及到知识仅供学习和参考，不得用于其他用途。

2 相关概念

（1）社会工程学

社会工程学在上世纪60年代左右作为正式的学科出现，广义社会工程学的定义是：建立理论并通过利用自然的、社会的和制度上的途径来逐步地解决各种复杂的社会问题，经过多年的应用发展，社会工程学逐渐产生出了分支学科，如公安社会工程学和网络社会工程学。社会工程学产生是一种通过对受害者心理弱点、本能反应、好奇心、信任、贪婪等心理陷阱进行诸如欺骗、伤害等危害手段取得自身利益，已成上升甚至滥用的趋势，成为计算机犯罪团伙实施犯罪的主要手段之一。

（2）社会工程学工具包SET

社会工程学工具包是一个叫devolution的项目，随着BackTrack发布被用来做渗透测试。在实施渗透的过程中，除了在发现软硬件的漏洞并实施攻击之外，最有效的方法就是洞察对方的思想，并获得所有与之相关的第一手信息。这个渗透技巧被叫做社会工程学攻击。于是被称之为SET的社会工程学工具包诞生了。

（3）传染性媒体生成器

传染性媒体生成器是一个相对简单的攻击向量，通过这个向量，SET生成一个文件夹，可以将这个文件复制到CD/DVD光盘上或是其他存储器上。一旦这些存储媒介插入到目标主机上，Autorun.inf这个文件就会自动加载，并运行Autorun.inf文件内指定的任意攻击。目前，SET支持加载可执行文件，同时也支持文件格式漏洞进行渗透攻击。

（4）隐藏木马

上述第3步中生成的木马文件如果不经过任何处理将会被用户发现，从而对木马文件进行查杀处理，使得后期攻击工作没法进行，因此对木马文件进行隐藏、伪装是非常有必要的。一般隐藏、伪装木马文件的方式有以下几种：其一是作为系统文件隐藏，其二是伪装成其他文件，其三是藏于系统文件夹中。

3 入侵过程

本文使用BT5作为攻击机，IP地址为192.168.5.114，XP系统作为靶机，IP地址为192.168.5.163，整个准备工作和入侵过程将分8个步骤进行，具体如下。（1）查看攻击机和靶机IP地址，在攻击命令行中输入ifconfig命令得到其IP为192.168.5.114，在靶机中DOS中输入ipconfig命令得到其IP地址为192.168.5.163，下文中将会用到上述2个IP地址。（2）进入攻击机系统，先切换路径，再启动社会工程学工具包SET。（3）从菜单中选择1号菜单，即选择SET，使用社会学工具包来完成攻击。（4）从菜单中选择3号菜单“传染性媒体生成器”实施攻击。（5）从菜单中选择2号菜单“Metasploit的执行标准”。（6）从菜单中选择2号菜单“受害者的Meterpreter shell寄回给攻击者”。（7）从菜单中选择16号菜单“后门程序”，试图绕过AV编码，系统会自动在SET目录下生成一个antorun的文件夹，此文件夹下面有个autorun.exe的可执行文件，可以将次文件修改个很具有诱惑力的名称来吸引用户来点击执行它，还可以考虑修改文件图标。（8）输入yes，启动监听应用程序。

通过上述8个步骤后，监听应用程序handler将会自动启动，等待鱼儿上钩，如何将此可执行文件传递出去，又如何让接受者心甘情愿执行此文件呢？下面将列举出几种常见的办法。（1）将生产的可执行文件复制到U盘或是光盘中，设置为自动启动。（2）将文件以邮件的方式发送出去，诱导用户下载并执行可执行文件。（3）将可执行文件上传到网上，诱导用户下载并执行。当有用户执行上述可执行文件时，系统会出现提示信息，提示攻击者有鱼儿上钩了。一个IP地址为192.168.5.163用户已经中招了，此用户就是上文中提到的靶机，接下来输入sessions-i，来查看会话信息，如果有多条鱼上钩，会话中将会一一列举出来。输入sessions－i 1选择1号会话，取得meterpreter会话权，表示已经取得了靶机的控制权。输入sysinfo来查看靶机系统信息，得到的结果确实是上文中提到的XP系统靶机，表示实验成功，另外还可以输入ipconfig等其他DOS命令来确认是否是靶机，这里就不演示了。

如果得到的权限不是最高权限，可以考虑提权，最后清除痕迹以免被用户发现，留下后门以便以后再次光临。接下来就可以获取本机中的敏感信息，比如通过破解系统的hash文件来获取系统的账号和密码等信息，如果靶机是一台服务器，那就可以获取其他更有价值的信息。

4 预防措施

传染性媒体生成器危害巨大，下面将提出几点预防建议。（1）禁用自动播放功能。（2）不要点击陌生移动介质中的可执行文件，俗话说好奇害死猫。（3）网上下载文件的时候，通过观察文件容量大小，文件名称等，留意其下载的对象是不是我们需要的文件，很有可能是其他恶意插件。

参考文献

[1]诸葛建伟,陈力波,田繁.Metasploit渗透测试魔鬼训练营[J].中国科技信息,2013(20):60.

[2]冯刚,梁妙园,陆学斌,魏开平.通用交互式多媒体应用系统生成器 IGMS[J].多媒体世界,1995,4-5,8.

作者简介：黄长江（1982-），男，湖北武汉，硕士，讲师，云技术和网络安全。

詹柳春，1984年12月，女，汉，广东省湛江市，本科，讲师，主要研究：云计算。