山东大学 软件 学院

信息安全导论 课程实验报告

|  |  |  |  |
| --- | --- | --- | --- |
| 学号：201600301079 | 姓名： 崔玉峰 | | 班级： 2016级软件4班 |
| 实验题目： 实验七HTML/VBScript脚本病毒 | | | |
| 实验学时：4 | | 实验日期： 2018/ | |
| 实验目的： 实验目的 学习脚本病毒的工作原理，举一反三，从而了解一般的二进制病毒的传播（而不是危害）机制。 实验内容 史上造成严重损失的病毒事件中，脚本病毒占了很大比例，如梅丽莎（）病毒和爱虫病毒等。  学习和分析：   |  |  | | --- | --- | | 教学例子1  //演示vbs脚本病毒（口令是“123”） |  | | 欢乐时光(VBS.happytime)病毒分析  //使用了加密手段 |  | | 梅利莎 (Melissa)病毒  //史上最严重的脚本病毒 | 样本自己找 | | 爱虫 (iloveyou)病毒  //史上次严重的脚本病毒 | 样本自己找 |   另外，建议找一个当下正流行或刚爆发的病毒，以linux上的脚本bash脚本病毒为推荐，比如Linux.BtcMine.174，尝试观察一下其运作机制。 | | | |
| 硬件环境：  PC  CPU : intel-i5  RAM: 8G | | | |
| 软件环境：  虚拟机：VMWARE  操作系统：Windows Xp sp3 | | | |
| 实验步骤与内容：     1. **演示VBS脚本病毒** 2. **虚拟机中运行WindosXP sp3系统，并且关闭防火墙程序。** 3. **将测试的程序vi-12：30v0.1.htm导入并修改文件夹路径**      1. **创建一个待感染的程序cyftest.htm**        1. **用IE打开程序vi-12：30v0.1.htm，无视警告继续：**      1. **虽然什么提示都没有但是cyftest.htm文件已经被病毒感染增加了一段病毒程序：**          1. **欢乐时光脚本病毒**   欢乐时光病毒是一种VBS脚本病毒，被病毒感染后会产生大量的Folder.htt文件，并且可以通过电子邮件进行传播是非常恶劣的病毒：   1. **查看欢乐时光病毒源码：**   需要查看隐藏文件才能查看，并且VBS病毒部分已经被加密，查看了很多文章都没有给出解密方法      通过查找还是找到了未加密的欢乐时光病毒源码：      通过阅读源码还是能得知此病毒基本的感染过程和传播形式的，它通过内嵌的VB脚本，可以在浏览网页时自动执行。首次染毒会将WINDOWS / WEB文件夹里的所有网页文件染上病毒，并向任何的EMAIL地址发送病毒邮件，只要感染了病毒就会在特殊的时间发作传播，并删除系统的重要文件exe,dll使系统瘫痪是非常恶劣的病毒，所以也证明VBS非常不安全。从网页中内嵌VBS脚本执行是非常危险的。           1. **梅丽莎病毒：**   该病毒通过电子邮件的方式传播，当用户打开附件中的“list.doc”文件时。将立刻感染病毒由VBA脚本编写，开创了此类病毒的先河病毒通过对注册表进行修改，并调用0utIook发送含有病毒的邮件，进行快速传播。由于该病毒发送的邮件的发件人是用户熟悉的，因此往往被很多人忽视。同时，该病毒会自动重复以上的动作，由此引起连锁反应，在短时间内，造成邮件服务器的大量阻塞，严重影响正常网络通讯。     1. **爱虫病毒：**   与梅丽莎病毒非常相似，都是通过电子邮件的方式进行传播，由VBS脚本编写，因发送的邮件主题为“I LOVE YOU” 而得名，一旦在Microsoft Outlook里打开这个邮件，病毒会自动复制自身代码到附件中并向地址簿中的所有邮件电址发送这个附件，修改注册表运行病毒代码。         1. **脚本病毒总结：**  通过学习和总结，发现以上的脚本病毒有很多的共同点，他们普遍通过邮件进行传播，可以用到html中执行VBS代码而大量的传播，并且编写简单，一个破坏力很强的病毒可能核心的代码量200行。病毒的执行过程也基本相同，主要分为传播和破坏两个部分，传播主要靠VBS将自己的代码拼接到其他网页上，破坏时很多样但是常常会破坏操作系统文件，并且有时时隐时现，通过代码随机破坏，让被感染的机器摸不着头脑；并且会更改系统的注册表使病毒可以自行启动。 但是到今天操作系统对于脚本病毒的监控已经有了很大的进步，并且主流的浏览器已经不在支持VBS代码，已经很少有大面积的脚本病毒爆发，所以只要按时更新系统，正确上网就可以尽量避免感染病毒 | | | |
| 结论分析与体会：    对于本次测试执行了演示病毒，欢乐时光病毒；并且查看了网络上爱虫病毒的源码分析了他们的作用机理，传播途径，作用特点等信息。因为近年来互联网，安全技术的快速发展， 今天操作系统对于脚本病毒的监控已经有了很大的进步，并且主流的浏览器已经不在支持VBS代码，已经很少有大面积的脚本病毒爆发，所以只要按时更新系统，正确上网就可以尽量避免感染病毒 | | | |