文章编号:1005-6033(2009)30-0081-03 收稿日期:2009-09-07

宏病毒感染过程及防范措施研究

梁 玲

(山西工程职业技术学院,山西太原,030009)

摘 要:宏病毒是利用MS Office中提供的VBA编程接口,专门制作的具有病毒特点的宏,这种病毒宏破坏办公文档,危害办公文档的安全。分析了宏病毒的感染过程及危害,提出了宏病毒的检测和防范方法。

关键词:宏病毒;病毒攻击;病毒感染;文档安全

中图分类号:TP393.08 文献标识码:A

可执行文件容易带毒已是众所周知,大家不会随便运行不了解的可执行文件。可是日常办公大量使用的Word和Excel文档也含有一种病毒(宏病毒),并且这些病毒可以自我复制、破坏文件,对此人们却不大了解。出于对这种病毒的警惕心低,宏病毒在人们大量使用的Word和Excel等办公文档中迅速传播,对人们的无纸化办公带来了威胁。因此,我们有必要了解宏病毒的发作机制及针对宏病毒的防治方法,增强办公文档的安全性。Word和Excel文档的宏病毒感染机制相似,本文以Word文档为例介绍宏病毒的感染过程及防治措施。

1 模板及宏机制

不论是Word还是Excel文档的创建都是通过模板来建立的,模板是为了形成最终文档而创建的特殊文档。模板包括如下一些元素:菜单、宏、格式等。模板是文本、图形和格式编排的蓝图。

Word提供了几种常规文档类型的模板,如商务信件、报告和备忘录。可以直接使用模板也可以自定义模板来创建新文档。默认情况下,Word自动基于公用模板Normal.dot创建文档。模板作为文档的基类,文档继承模板的属性,包括宏、菜单及格式等。

Word提供强大的宏功能,宏是组织到一起的一系列命令的集合,宏使日常工作变得简单。Word启动时会自动加载Normal.dot模板,其中含有设置好的宏。可以为宏指定特定的名称,以标示其为自动宏,在执行某项操作时,如启动Word、打开文档时就自动执行拥有特殊命名的宏。Word可以识别以下自动宏:AutoExec(启动Word)、AutoNew(新建文档)、AutoOpen(打开文档)、AutoClose(关闭文档)、AutoExit(退出Word)。

宏病毒主要寄生在以下3个宏中:AutoOpen,AutoNew,AutoClose。带毒文档打开时,将宏病毒写入公用模板(Normal.dot)中,再由公用模板传染给其他正常的文档[1]。

2 病毒感染机制

此处以MorthersDayVirus为例研究宏病毒感染机制。MothersDayVirus感染Word文档和Normal.dot模板,被感染的Word文档打开或关闭时会首先弹出一个对话框,在对话框关闭时将控制权转移给正常的Word执行。MothersDayVirus使用Document_Open宏(文档打开时执行)感染Normal.dot,使用AutoClose自动宏感染其他文档。

MothersDayVirus病毒执行流程如下[3]:

(1)判断当前文档和Normal.dot是否感染;

(2)如Normal.dot未被感染,则清空Normal.dot,并将病毒复制到Normal.dot,同时,将宏重命名为AutoClose;

(3)如果当前文档未被感染,则清空当前文档宏命令,并将病毒复制到当前文档,同时将宏重命名为Document_Open;

(4)禁用Word的宏编辑功能;

(5)添加自动保存功能;

(6)病毒发作执行特定操作;

(7)返回到程序正常路径执行。

3 Microsoft Word对象

Application对象表示Word应用程序本身。可以从Application对象访问Word公开的所有对象和集合及Application自身的属性和方法。在编辑一个Word文档时,同时也创建了一个Application对象。用户可以通过该对象控制或获取应用程序属性。

Application对象的一些属性控制着应用程序的外观。如,设置DisplayStatusBar=True,则状态栏可见;设置WindowStata=wdWindowStateMaxmize,则应用程序窗口处于最大化状态。

Application对象的属性也可访问低级的对象,比如,Windows集合(当前所有打开的窗口)和Documents集合(当前所有打开的文档)。从对象层次中高一级的对象可以访问到低级的对象。如:可以使用以下实例来打开一个文档。

Application.Documents.Open FileName :="C:\DOC1.DOC"

(1)运用Document对象。可以使用Document对象或Documents集合的属性和方法打开、创建、保存或关闭文件。

(2)返回Document对象。可以使用Documents(index)返回文件对应的Document,index是该文档的名字或索引号(该文档在集合中的位置)。示例如下:

Set myDoc = Documents("Mydoc.doc")

用户添加或关闭文档时,某个文档的索引号会发生变化,因此使用名字更加稳定。

(3)打开文档。Set myDoc = Documents.Open (FileName := "TEST.DOC")

(4)关闭文档。Documents("mydoc.doc").Close。如果对文档进行过修改,Word会提示是否保存所做的修改。用户可以设置SaveChanges参数wdDoNotSaveChanges或wdSaveChanges常量来使该提示不再出现。

Documents("mydoc.doc").Close SaveChanges :=wdSaveChanges

(5)向文档添加对象。可以使用Add方法向文档中添加表格、图片、脚注等对象。

ActiveDocument Tables. Add Range :=myRange, NumRows :=3,

NumColumns :=3

(6) 修改 Word 命令。在“工具”菜单->“宏”->“宏的位置”(选择“Word 命令”)。在“宏名”文本框中,选中要修改的 Word 命令(如 FileSave),在“宏的位置”下拉框中选择要保存宏的模板或文档。如,选择 Normal.dot 创建一个共用宏(FileSave 会自动对所有文档进行修改)。如下所示:

ActiveDocument.Save ′保存活动文档或模板。

(7) 保存活动文档或模板。可以在 FileSave 过程中添加命令或删除已有的 ActiveDocument.Save 命令。FileSave 命令每次运行时,FileSave 宏都将执行,要恢复原有的 FileSave 命令,需更改 FileSave 宏。

此外,可以创建与 Word 命令同名的过程,使用名为“Main”的例程替换 Word 命令。

(8) Document 事件。打开文档时发生 Open 事件,关闭文档时发生 Close 事件。一个文档事件的范围取决于它保存的位置,在文档中保存的事件仅随文档激活,在模板中保存的事件随所有文档及模板自身而激活。一个 FileNew 过程必须保存在模板中,保存在文档中的 FileNew 事件不会运行。

宏病毒通常有 3 种激发机制:利用自动运行的宏;修改 word 的命令;使用 document 对象的事件。

4　宏病毒检测与防范

若在处理 Word 或 Excel 文档时发现以下一些问题,有可能是中了宏病毒[3]。

在 word “宏”菜单下,点击通用模板(Normal.dot),发现有“AutoOpen”等自动宏,“FileSave”等文件操作宏或一些名字奇怪的宏,而自己又没有加载特殊模板。

如发现打开一个文档,它未经任何改动,立即就有存盘操作;

文档只能以模板方式存盘。

对宏病毒的防范有以下一些措施[4]。

备份干净的通用模板(Normal.dot),染毒后还原 Normal.dot 文件。

保留文档中宏清单,及时核对哪些宏不是系统宏也不是自制宏,及时予以删除。

结合数字签名启用宏。

使用杀毒软件清除宏病毒。

5　使用 VBA 和 VBS 创建杀毒宏

宏可以被利用以携带病毒,同时我们也可以利用宏来杀毒,此处展示了杀毒宏的制作[5]。

(1) 使用 VBA 杀毒。通过宏的 VBA 代码恢复被病毒篡改的设置,然后删除病毒宏和杀毒宏本身。查看一下 MothersDay 宏病毒的攻击部分。

Application.CommandBars ("Tools") .Enabled=False ′禁用“工具”菜单按钮。

Application.CommandBars ("Macro") .Enabled =False ′禁用“宏”菜单按钮。

Index=1

Do ′禁用“宏”菜单中的所有按钮。

Application.CommandBars (“Macro”) .Controls (Index) .Enabled=False

Loop while Index <=Application.CommandBars (“Macro”) .Controls.Count

Msgbox Prompt:=“你的计算机已感染母亲节病毒!”,Title:=“计算机感染母亲节病毒”。

可以得知,MothersDay 病毒的篡改设置包括:禁用“宏”菜单按钮、禁用“工具”菜单按钮、禁用“Visual Basic”工具栏,在打开或关闭染毒文档时弹出消息框。

病毒体注入文档之后,MothersDay 将 Word 对象名称改为“MothersDay”,如下所示:

NormalTemplate.VBProject.VBComponents.Item (1) .Name = “Virus Name”

要恢复这些设置,只要创建杀毒宏并将上述代码中的“False”值都改为“True”,并将 Mircosoft Word 对象名改回“ThisDocument”即可。恢复设置后再将病毒宏和杀毒宏一起删除。在删除宏病毒时,要注意分别删除模板和当前活动文档中的病毒宏代码。

```
Dim i as Object, a as Integer
For Each i in NormalTemplate.VBProject.VBComponents
a=i.Code.Module.CountOfLines
i.CodeModule.DeleteLines 1,a
Next
ActiveDocument.Save
```

总结杀毒宏的基本结构为:恢复设置,删除模板中的病毒,删除活动文档中的病毒,保存文档。杀毒宏编写完成后添加至病毒宏末尾,运行此病毒即可删除 MothersDay 病毒。

(2) 使用 VBS 杀毒。使用 VBS 脚本语言根据病毒标记可以判断文档是否被感染,若感染病毒则向此文档中写入杀毒宏并运行以将病毒清除。

首先要将杀毒宏代码写入字符串中,等待被写入。在写入字符串时要使用转义字符,如换行符要用“vbCr”替代,双引号要用“Chr (34) ”来代替,字符串之间要用“&”来连接。

```
“Private Sub killVirus() ” & vbCr & _
“Application.CommandBars (“ +Chr (34) +”Tools “+Chr (34) +”) .Enabled = True” & vbCr & _
“Application.CommandBars (“ +Chr (34) +”Macro “+Chr (34) +”) .Enabled = True” & vbCr & _
```

以上代码假定杀毒宏的名字是“killVirus”,所有字符都有放入双引中,“vbCr & _”为换行标志,这样使得宏代码在 VBS 脚本中更清晰。宏代码字符串间不能有空行或注释。

创建一个“Word.Application”对象,设定对象名为“word_app”,打开文档时不可见。

```
Set word_app=CreateObject (“Word.Application”)
word_app.Visible = False
Set doc=word_app.Documents.Open (“D:\ll\MacroVirus\defaced.doc”)
```

如有病毒感染标记,则向染毒文档中写入杀毒宏并运行。

```
doc.VBProject.VBComponents(1) .CodeModule.AddFromString strMacro
word_app.Run killVirus
```

6　结语

经过对宏病毒感染过程的详细分析,可以找出检测及预防宏病毒的方法,甚至可以制作杀毒宏清除宏病毒。宏病毒的变种非常容易制作,用户应加强对宏病毒的了解,综合运用各种预防及杀毒措施避免宏病毒发作,保护日常办公文档的安全性。

参考文献

[1]　张仁斌,李钢,侯整风.计算机病毒与反病毒技术[M].北京:

文章编号:1005-6033(2009)30-0083-03 收稿日期:2009-08-26

浅谈 IT 技术类博客

马 珺

(南京森林公安高等专科学校,江苏南京,210046)

摘 要:阐述了技术博客的定义、特点以及发展的现状,认为技术博客不仅是博主表达个人思想的空间,也成了技术人员在互联网上交流工作经验与研究技术的辅助手段。

关键词:技术博客;专业博客;互联网

中图分类号:TP393 文献标识码:A

在互联网世界当中,博客的迅速发展和网民的广泛参与,使博客种类趋于多元化、内容形式多样化。

Technorati 的《2008 全球博客状态报告》中,Technology 作为关键词的博客就占了 46%,技术博客不仅是博主表达个人思想的空间,也成了技术人员在互联网上交流工作经验与研究技术的辅助手段。

1 技术博客定义

目前,人们习惯把 IT 技术、教育技术、军事技术等专业技术性较强的博客归入技术博客一类。特别是 IT 技术类博客的兴起,已成为众多 IT 技术人员网上分享技术成果、传播知识经验的重要平台。本文尝试对与技术博客相近的几类博客的内涵和外延进行比较分析,以期能得到一个较为具体的技术博客的定位。

1.1 专业博客与技术博客

专业博客产生的重要原因就是用户个性化、多样化需求的不断增长,它是建立在彻底大众化博客交流的基础之上。相对于一般博客、大众博客而言,它所涉及的圈子较小,往往是从一个较专业的角度来关注这个领域的一举一动、追踪最新动态、提炼专业信息,并通过别人的反馈和评论不断修正自己的思想。例如记者博客、财经博客、图情博客等。

与专业博客相同,技术博客的创建者一般都是比较关注于某一专业技术领域,并且对这个领域有着比较深入的了解和研究,其博客收录的内容大多是关于该领域的文献,这就使该博客群的知识深度大为加强。技术博客上主要公布博主的学习心得、工作体验、研究成果,甚至会邀请这方面的专家、学者、权威人士将他们的探索方式、研究思路、实验方法、学习经验等,通过双向交流沟通和内容精确归类,以实现知识的交互性和更加微观的知识聚类,并且能够精确地传达给目标用户。

可见,两类博客有很多共通之处,而专业博客的外延更广一些,它不单单强调专业技术,更是突破了职业的划分,根据社会多元的方方面面,涉足不同领域的专业分类,只要是旨在介绍或者探讨某一领域相关知识或者学术的博客都可以归入专业博客之中。

1.2 科普博客与技术博客

科普博客作为博客家族的衍生部落,具有科学化、交互化、序列性和非商业性等特征,通过互联网这种方式,将科学知识向大众进行推广和传播的新兴方式。此类博客的博主多为民间科学家,为科学的普及、科技的传播提供了"寓教于乐"的可能。由此也可以看出,科普博客所面对的受众仍然是广大的互联网用户,他们不一定要具有哪一方面的专业知识,却仍然可以从科普博客中吸收知识,进行交流。

技术博客的博主可能只是一个普通的从事或者精通某一技术领域的技术人员。这类博客的写作目的更多是一个自身的知识积累和管理,虽然他们的博文也起到了科技知识的传播推广等作用,但是专业技术性质更强,其所面对的受众不可能是整个互联网用户,而是某一个技术用户群体。可见,这两类博客虽然

清华大学出版社,2006.

[2] 秦志光,张凤荔.计算机病毒原理与防范[M].北京:人民邮电出版社,2007.

[3] 张庆华.网络安全与黑客攻防宝典[M].北京:电子工业出版社,2007.

[4] 王鑫.基于 Word 宏病毒的识别及防治方法[J].电脑与电信技术,2005(2):63-67.

(责任编辑:郑 光)

第一作者简介:梁 玲,女,1971 年生,2007 年毕业于中北大学计算机应用专业(硕士),讲师,山西工程职业技术学院网络中心,山西省太原市,030029.

A Research on Infecting Process and Prevention Approach of Macro Virus

LIANG Ling

ABSTRACT: Macro virus is a kind of macro bearing the characteristics of virus, which exploits the VBA programming interface provided by MS Office. Macro virus destroys office documents, can self-copy and spread through document. This paper gives detailed analysis on infecting process of macro virus and its danger, and puts forward the testing method of macro virus and preventing approach.

KEY WORDS: macro virus; attack; infecting; document safety