恶意代码的详细介绍

- ✓ 出处：站长百科
- ✓ 原文地址：http://www.zzbaike.com/wiki/恶意代码
- ✓ 本电子书整理自站长百科恶意代码词条，查看内容请访问网站

目录

✓ *出处：站长百科*
✓ *原文地址：http://www.zzbaike.com/wiki/恶意代码*
✓ *本电子书整理自站长百科恶意代码词条，查看内容请访问网站*

恶意代码（Unwanted Code）是指没有作用却会带来危险的代码，一个最安全的定义是把所有不必要的代码都看作是恶意的，不必要代码比恶意代码具有更宽泛的含义，包括所有可能与某个组织安全策略相冲突的软件。

恶意代码的特征

恶意代码或者叫恶意软件具有如下共同特征：

- 恶意的目的
- 本身是程序
- 通过执行发生作用

有些恶作剧程序或者游戏程序不能看作是恶意代码。对滤过性病毒的特征进行讨论的文献很多，尽管它们数量很多，但是机理比较近似，在防病毒程序的防护范围之内，更值得注意的是非滤过性病毒。

非滤过性病毒

非过滤性病毒包括口令破解软件、嗅探器软件、键盘输入记录软件，远程特洛伊和谍件等等，组织内部或者外部的攻击者使用这些软件来获取口令、侦察网络通信、记录私人通信，暗地接收和传递远程主机的非授权命令，而有些私自安装的P2P软件实际上等于在企业的防火墙上开了一个口子。 非滤过性病毒有增长的趋势，对它的防御不是一个简单的任务。与非过滤性病毒病毒有关的概念包括：

谍件

谍件（Spyware）与商业产品软件有关，有些商业软件产品在安装到用户机器上的时候，未经用户授权就通过Internet连接，让用户方软件与开发商软件进行通信，这部分通信软件就叫做谍件。用户只有安装了基于主机的防火墙，通过记录网络活动，才可能发现软件产品与其开发商在进行定期通讯。谍件作为商用软件包的一部分，多数是无害的，其目的多在于扫描系统，取得用户的私有数据。

远程访问特洛伊

远程访问特洛伊RAT 是安装在受害者机器上，实现非授权的网络访问的程序，比如NetBus 和SubSeven 可以伪装成其他程序，迷惑用户安装，比如伪装成可以执行的电子邮件，或者Web下载文件，或者游戏和贺卡等，也可以通过物理接近的方式直接安装。

Zombies

恶意代码不都是从内部进行控制的，在分布式拒绝服务攻击中，Internet的不少 站点受到其他主机上 zombies程序的攻击。zombies程序可以利用网络上计算机系统的安全漏洞将自动攻击脚本安装到多台主机上，这些主机成为受害者而听从攻击者指挥，在某个时刻，汇集到一起去再去攻击其他的受害者。

破解和嗅探程序和网络漏洞扫描

口令破解、网络嗅探和网络漏洞扫描是公司内部人员侦察同事，取得非法的资源访问权限的主要手段，这些攻击工具不是自动执行， 而是被隐蔽地操纵。

键盘记录程序

某些用户组织使用 PC 活动监视软件监视使用者的操作情况，通过键盘记录，防止雇员不适当的使用资源，或者收集罪犯的证据。这种软件也可以被攻击者用来进行信息刺探和网络攻击。

P2P系统

基于Internet的点到点 （peer-to-peer）的应用程序比如 Napster、Gotomypc、AIM 和 Groove，以及远程访问工具通道像Gotomypc，这些程序都可以通过HTTP或者其他公共端口穿透防火墙，从而让雇员建立起自己的VPN，这种方式对于组织或者公司有时候是十分危险的。因为这些程序首先要从内部的PC远程连接到外边的Gotomypc 主机，然后用户通过这个连接就可以访问办公室的PC。这种连接如果被利用，就会给组织或者企业带来很大的危害。

逻辑炸弹和时间炸弹

逻辑炸弹和时间炸弹是以破坏数据和应用程序为目的的程序。一般是由组织内部有不满情绪的雇员植入， 逻辑炸弹和时间炸弹对于网络和系统有很大程度的破坏.

恶意代码的传播手法

恶意代码编写者一般利用三类手段来传播恶意代码：软件漏洞、用户本身或者两者的混合。有些恶意代码是自启动的蠕虫和嵌入脚本，本身就是软件，这类恶意代码对人的活动没有要求。一些像特洛伊木马、电子邮件蠕虫等恶意代码，利用受害者的心理操纵他们执行不安全的代码；还有一些是哄骗用户关闭保护措施来安装恶意代码。

利用商品软件缺陷的恶意代码有Code Red 、KaK 和BubbleBoy。它们完全依赖商业软件产品的缺陷和弱点，比如溢出漏洞和可以在不适当的环境中执行任意代码。像没有打补丁的IIS软件就有输入缓冲区溢出方面的缺陷。利用Web 服务缺陷的攻击代码有Code Red、Nimda，Linux 和Solaris上的蠕虫也利用了远程计算机的缺陷。

恶意代码编写者的一种典型手法是把恶意代码邮件伪装成其他恶意代码受害者的感染报警邮件，恶意代码受害者往往是Outlook地址簿中的用户或者是缓冲区中WEB页的用户，这样做可以最大可能的吸引受害者的注意力。一些恶意代码的作者还表现了高度的心理操纵能力，LoveLetter 就是一个突出的例子。一般用户对来自陌生人的邮件附件越来越警惕，而恶意代码的作者也设计一些诱饵吸引受害者的兴趣。附件的使用正在和必将受到网关过滤程序的限制和阻断，恶意代码的编写者也会设法绕过网关过滤程序的检查。使用的手法可能包括采用模糊的文件类型，将公共的执行文件类型压缩成zip文件等等。

对聊天室IRC（Internet Relay Chat）和即时消息IM(instant messaging)系统的攻击案例不断增加，其手法多为欺骗用户下载和执行自动的Agent软件，让远程系统用作分布式拒绝服务(DDoS)的攻击平台，或者使用后门程序和特洛伊木马程序控制之。

恶意代码传播的趋势

恶意代码的传播具有下面的趋势：

- 种类更模糊

恶意代码的传播不单纯依赖软件漏洞或者社会工程中的某一种，而可能是它们的混合。比如蠕虫产生寄生的文件病毒，特洛伊程序，口令窃取程序，后门程序，进一步模糊了蠕虫、病毒和特洛伊的区别。

- 混合传播模式

“混合病毒威胁”和“收敛（convergent）威胁”的成为新的病毒术语，“红色代码”利用的是IIS的漏洞，Nimda实际上是1988 年出现的Morris 蠕虫的派生品种，它们的特点都是利用漏洞，病毒的模式从引导区方式发展为多种类病毒蠕虫方式，所需要的时间并不是很长。

- 多平台

多平台攻击开始出现，有些恶意代码对不兼容的平台都能够有作用。来自Windows的蠕虫可以利用Apache的漏洞，而Linux蠕虫会派生exe格式的特洛伊。

- 使用销售技术

另外一个趋势是更多的恶意代码使用销售技术，其目的不仅在于利用受害者的邮箱实现最大数量的转发，更重要的是引起受害者的兴趣，让受害者进一步对恶意文件进行操作，并且使用网络探测、电子邮件脚本嵌入和其它不使用附件的技术来达到自己的目的。

恶意软件（malware）的制造者可能会将一些有名的攻击方法与新的漏洞结合起来，制造出下一代的 WM/Concept，下一代的 Code Red，下一代的 Nimda。对于防病毒软件的制造者，改变自己的方法去对付新的威胁则需要不少的时间。

- 服务器和客户机同样遭受攻击

对于恶意代码来说服务器和客户机的区别越来越模糊，客户计算机和服务器如果运行同样的应用程序，也将会同样受到恶意代码的攻击。象IIS服务是一个操作系统缺省的服务，因此它的服务程序的缺陷是各个机器都共有的，Code Red的影响也就不限于服务器，还会影响到众多的个人计算机。

- Windows 操作系统遭受的攻击最多

Windows操作系统更容易遭受恶意代码的攻击，它也是病毒攻击最集中的平台，病毒总是选择配置不好的网络共享和服务作为进入点。其它溢出问题，包括

字符串格式和堆溢出，仍然是滤过性病毒入侵的基础。病毒和蠕虫的攻击点和附带功能都是由作者来选择的。

另外一类缺陷是允许任意或者不适当的执行代码，随着scriptlet.typelib和Eyedog漏洞在聊天室的传播，JS/Kak利用IE/Outlook的漏洞，导致两个ActiveX控件在信任级别执行，但是它们仍然在用户不知道的情况下，执行非法代码。

- 恶意代码类型变化

此外，另外一类恶意代码是利用MIME边界和uuencode头的处理薄弱的缺陷，将恶意代码化装成安全数据类型，欺骗客户软件执行不适当的代码。

相关条目

- 黑客
- 蠕虫病毒

更多电子书

站长常用工具：

Alexa查询：http://alexa.zzbaike.com/ Alexa中文专题站

http://www.alexacn.org/alexa-faq.html Alexa工具条下载

关键词排名检索工具：http://keywordsrank.zzbaike.com/

在线FTP工具：http://webftp.zzbaike.com/

PR查询工具：http://pr.zzbaike.com/

关键词密度检测工具：http://keywords.zzbaike.com/

收录数量查询：http://indexed.zzbaike.com/

Whois查询：http://whois.zzbaike.com/

反向链接查询：http://linksincount.zzbaike.com/

Gzip查询工具：http://gzip.zzbaike.com

站长百科免费美国空间

freehost4life美国免费空间（http://www.freehost4life.com），服务器位于softlayer的达拉斯机房，是中国访问速度最快的美国主机之一。

站长百科 1 美元银币竞价活动

每周总共举行 3 次美元竞价：http://bbs.zzbaike.com/forum-45-1.html

SEO 优化教程

SEO 方面的知识有很多，对于新手来说，如果你不知道，不清楚这方面的知识，那么，你可以看看这两部搜索引擎指南：

SEO搜索引擎优化基础教程：http://bbs.zzbaike.com/thread-9952-1-1.html

SEO搜索引擎优化高级教程：http://bbs.zzbaike.com/thread-12692-1-1.html

WordPress 开发文档

wordpress的中文翻译文档http://www.wordpress.la/codex.html，wordpress开发的相关知识都有，对WordPress开发感兴趣的博主会有一定的用处。

WordPress免费主题：http://www.wordpress.la/theme.html

WordPress免费插件：http://www.wordpress.la/plugin.html

WordPress主题制作电子书：http://bbs.zzbaike.com/thread-9954-1-1.html

Apache2.2 中文文档电子书http://bbs.zzbaike.com/thread-9955-1-1.html

IXWeHosting 控制面板使用手册(在线版+PDF 电子书)

http://bbs.zzbaike.com/thread-9953-1-1.html

更多电子书下载：http://down.zzbaike.com/ebook/

视频教程：

1. 美国主机 IXWebHosting 使用视频教程（在线观看及下载）

   http://bbs.zzbaike.com/thread-47008-1-1.html

2. Godaddy 主机及域名使用视频教程（在线观看及下载）

   http://bbs.zzbaike.com/thread-50005-1-1.html

如果您有站长类电子书，请到这里与我们分享：

http://bbs.zzbaike.com/forum-69-1.html

详情见： http://bbs.zzbaike.com/thread-23156-1-1.html

站长百科感谢您下载阅读，多谢支持！