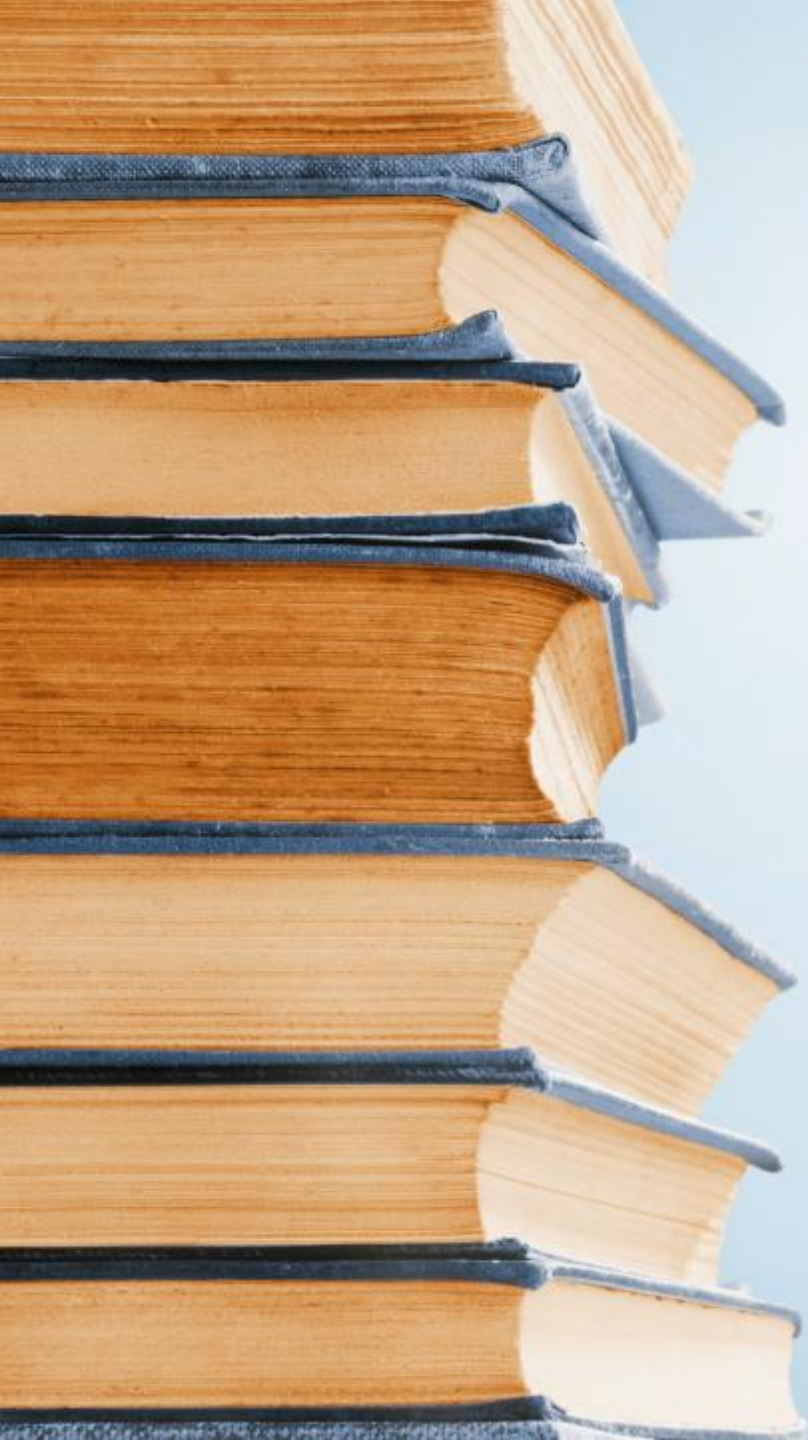


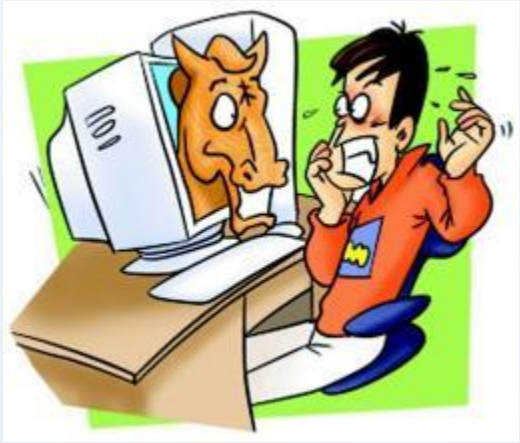
网络木马

计算机病毒

关于网络木马

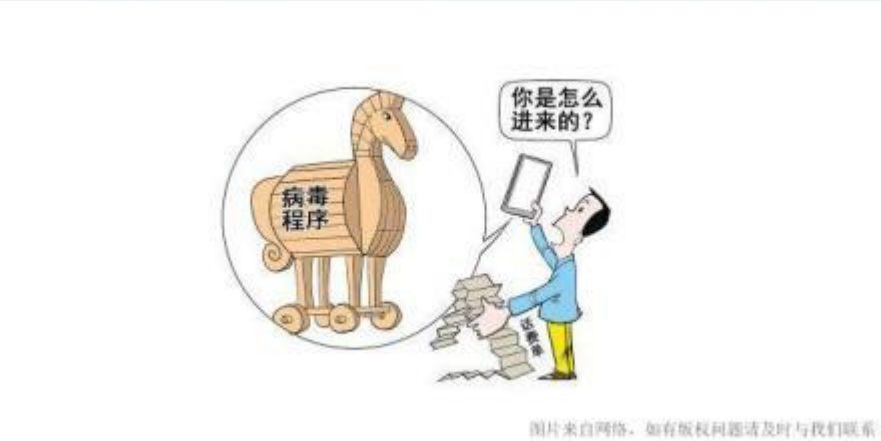
- 简介
- 病毒来源
- 应用领域
- 使用的技术
- 防范措施
- 实例

简介



木马病毒源自古希腊特洛伊战争中著名的“木马计”而得名，顾名思义就是一种伪装潜伏的网络病毒，等待时机成熟就出来“害人”。

木马来源



图片来自网络，如有版权问题请及时与我们联系

病毒传染方式

传染方式:通过电子邮件附件发出，捆绑在其他的程序中。当用户使用该程序，木马病毒便被激活，在特定的时间内使攻击者内更加容易地操控你的电脑。

病毒特性

病毒特性:会修改注册表、驻留内存、在系统中安装后门程序、开机加载附带的木马。

病毒破坏性

木马病毒的破坏性:木马病毒的发作要在用户的机器里运行客户端程序，一旦发作，就可设置后门，定时地发送该用户的隐私到木马程序指定的地址，一般同时内置可进入该用户电脑的端口，并可任意控制此计算机，进行文件删除、拷贝、改密码等非法操作

木马应用领域

1、系统病毒：

系统病毒的前缀为：Win32、PE、Win95、W32、W95等。这些病毒的一般公有的特性是可以感染windows操作系统的 *.exe 和 *.dll 文件，并通过这些文件进行传播。如CIH病毒。

2、蠕虫病毒：

蠕虫病毒的前缀是：Worm。这种病毒的公有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。比如冲击波(阻塞网络)，小邮差(发带毒邮件) 等。

木马应用领域

3、木马病毒、黑客病毒：

木马病毒其前缀是：Trojan，黑客病毒前缀名一般为 Hack 。木马病毒的公有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的电脑进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的电脑，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型都越来越趋向于整合了。一般的木马如QQ消息尾巴木马 Trojan.QQ3344 ，还有大家可能遇见比较多的针对网络游戏的木马病毒如 Trojan.LMir.PSW.60 。

4、脚本病毒：

脚本病毒的前缀是：Script。脚本病毒的公有特性是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码(Script.Redlof)——可不是我们的老大代码兄哦 ^_^。脚本病毒还会有如下前缀：VBS、JS(表明是何种脚本编写的)，如欢乐时光(VBS.Happytime)、十四日(Js.Fortnight.c.s)等。

木马应用领域

5、宏病毒：

其实宏病毒是也是脚本病毒的一种，由于它的特殊性，因此在这里单独算成一类。宏病毒的前缀是：Macro，第二前缀是：Word、Excel(也许还有别的)。该类病毒的公有特性是能感染OFFICE系列文档，然后通过OFFICE通用模板进行传播，如：著名的美(Macro.Melissa)。

6、后门病毒

后门病毒的前缀是：Backdoor。该类病毒的公有特性是通过网络传播，给系统开后门，给用户电脑带来安全隐患。如54很多朋友遇到过的IRC后门Backdoor.IRCBot 。

木马应用领域

7、病毒种植程序病毒Dropper
这类病毒的公有特性是运行时会从体内释放出一个或几个新的病毒到系统目录下，由释放出来的新病毒产生破坏。如：冰河播种者(Dropper.BingHe2.2C)、MSN射手(Dropper.Worm.Smibag)等。

8.破坏性程序病毒
破坏性程序病毒的前缀是：Harm。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒便会直接对用户计算机产生破坏。如：格式化C盘(Harm.formatC.f)、杀手命令(Harm.Command.Killer)等。

木马应用领域

9.玩笑病毒

玩笑病毒的前缀是：Joke。也称恶作剧病毒。这类病毒的公有特性是本身具有好看的图标来诱惑用户点击，当用户点击这类病毒时，病毒会做出各种破坏操作来吓唬用户，其实病毒并没有对用户电脑进行任何破坏。如：女鬼(Joke.Girlghost)病毒。

10.捆绑机病毒

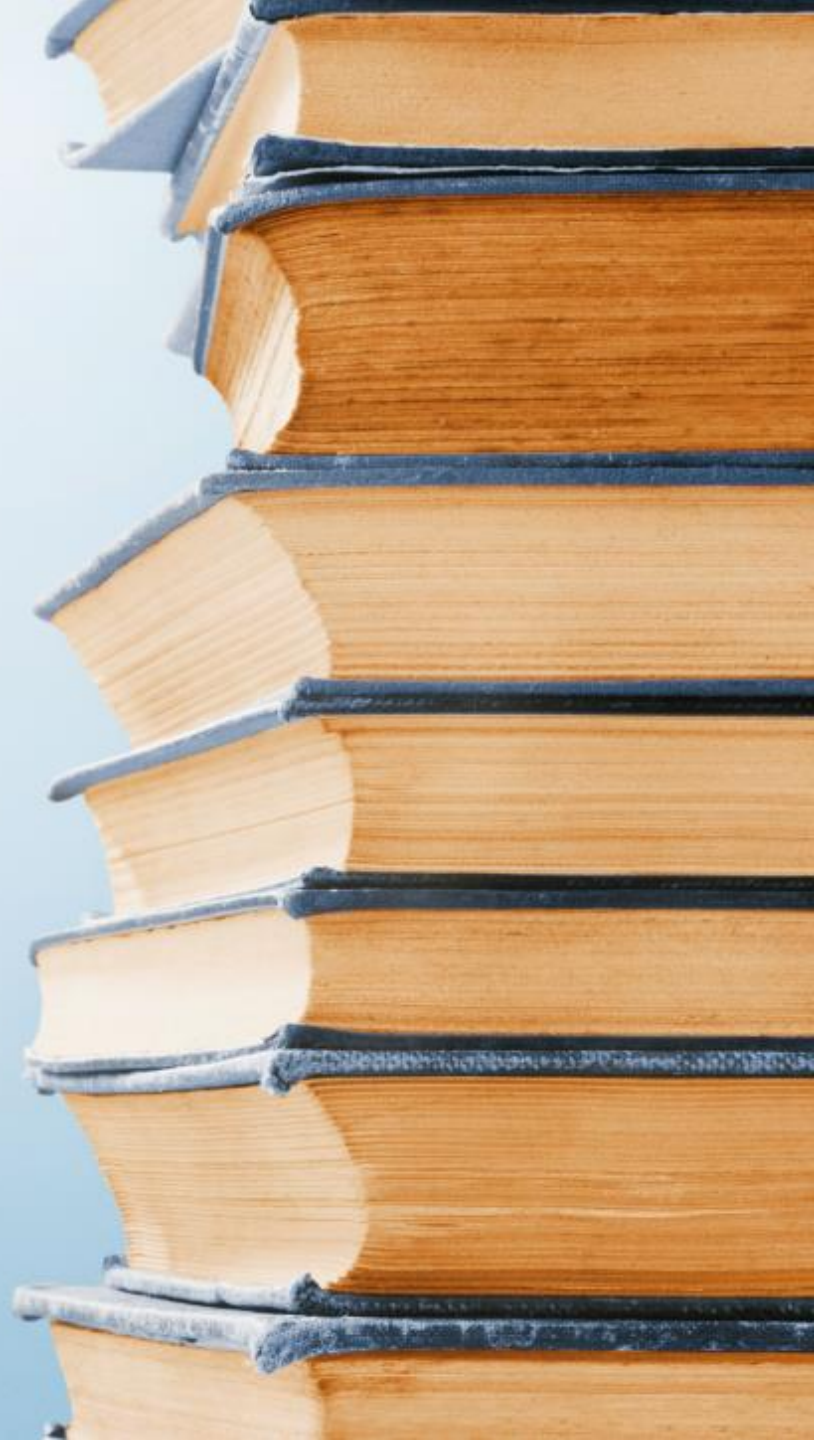
捆绑机病毒的前缀是：Binder。这类病毒的公有特性是病毒作者会使用特定的捆绑程序将病毒与一些应用程序如QQ、IE捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时，会表面上运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。如：捆绑QQ(Binder.QQPass.QQBin)、系统杀手(Binder.killsys)等。

使用的技术

1、了解一门高级语言（java，python，go等）

2、懂得服务器的搭建和运行维护的知识（灰鸽子）

3、会一些简单的加密技术

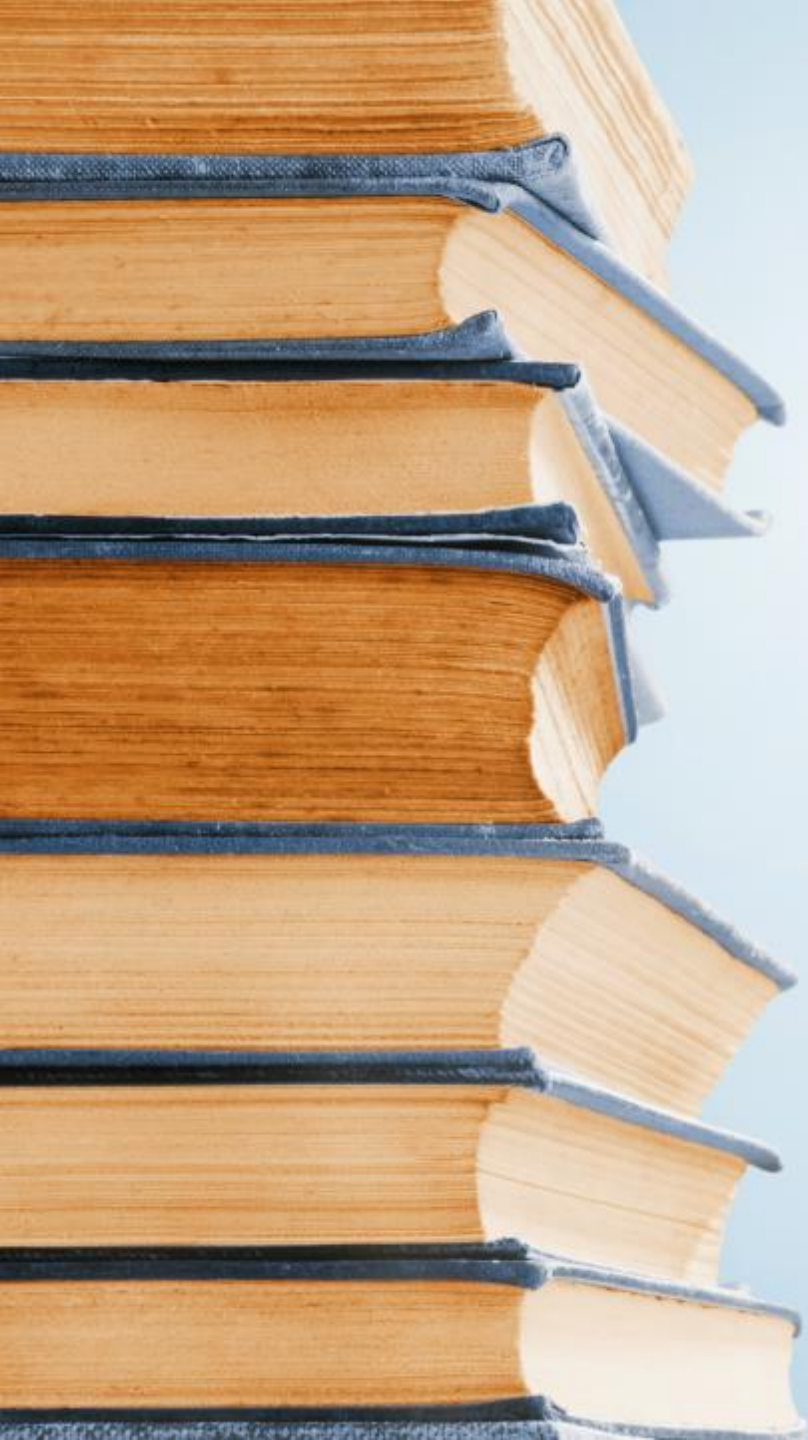


防范措施

1.安装杀毒软件（其实没用）和个人防火墙，并及时升级。
2.把个人防火墙设置好安全等级，防止未知程序向外传送数据。
3.可以考虑使用安全性比较好的浏览器和电子邮件客户端工具。
4.如果使用IE浏览器，应该安装卡卡安全助手，防止恶意网站在自己电脑上安装不明软件和浏览器插件，以免被木马趁机侵入。
5．不要执行任何来历不明的软件
6．不要随意打开邮件附件。现在绝大部分木马病毒都是通过邮件来传递的，而且有的还会连环扩散，因此对邮件附件的运行尤其需要注意。

实例

见我博客



Thanks