初识Trojan木马

四川师范大学/李敏
邮箱：limin@sicnu.edu.cn

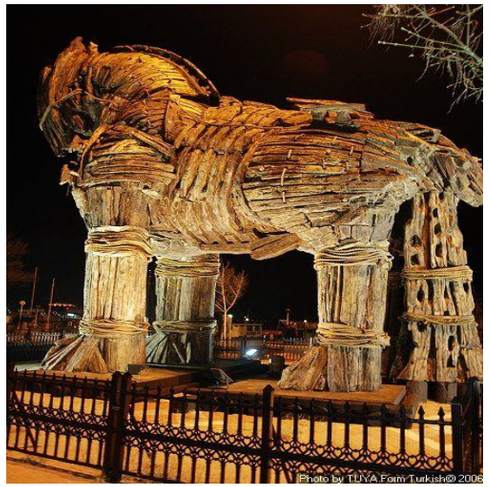
目 录

CONTENTS

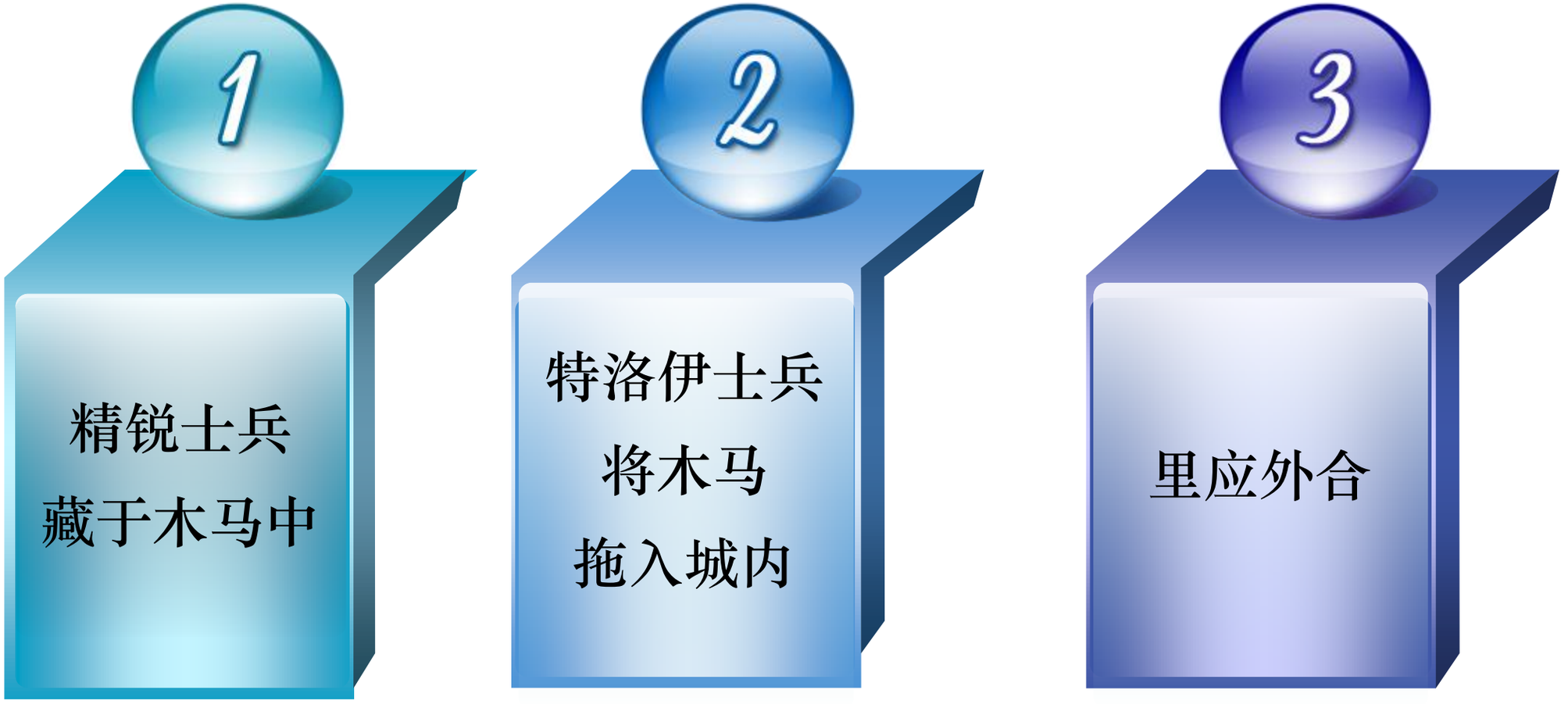
木马概念

木马概念

传说中的木马

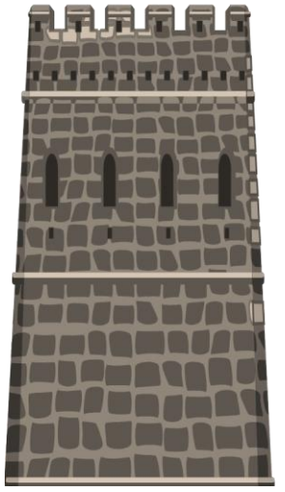


木马概念



木马概念

希腊军队



特洛伊城墙

黑　客

防火墙

控制

控制端

木马端

木马概念

定义

1. 一种隐蔽的远程控制工具
2. C/S结构的程序

02

章节

PART

木马特点

木马特点

1. 欺骗性
2. 隐蔽性
3. 非授权性

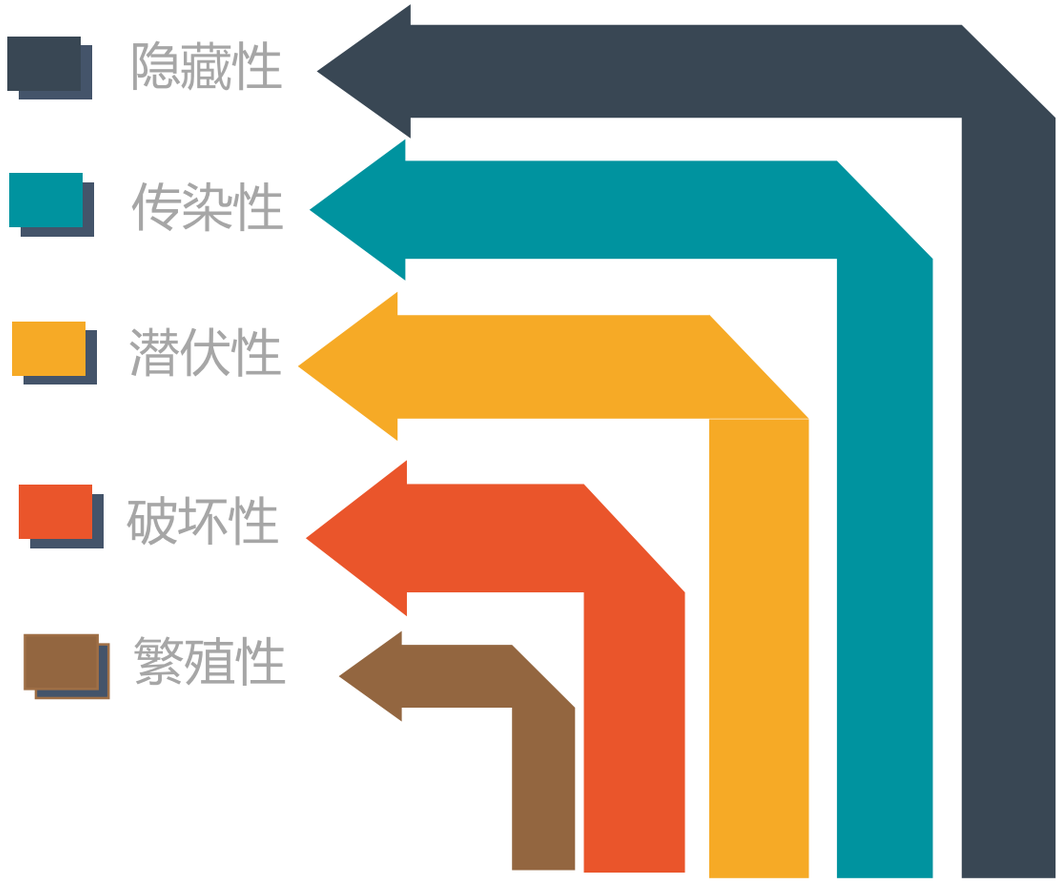
木马特点

木马：“一经进入，后患无穷”

有时又被称为“木马病毒”

木马特点

病毒



木马特点

病毒例子

熊猫烧香

勒索病毒

木马特点

木马：本身不带伤害性，没有感染力

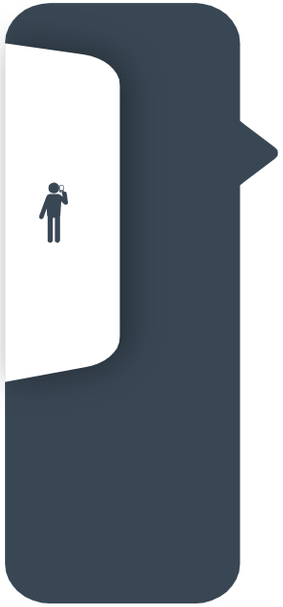
木马特点

木马程序企图

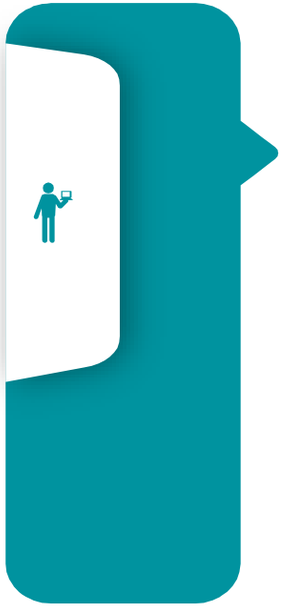
1. 非授权访问资源
2. 非授权访问资源
3. 更改或破坏系统和数据

木马特点

木马危害

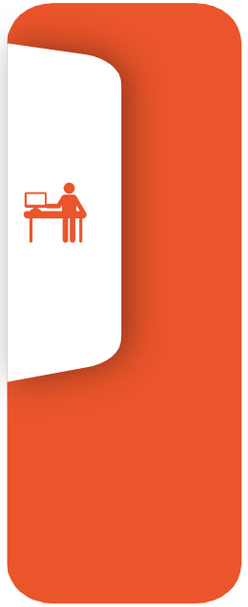


赤裸裸
受监视



敏感信息
机密泄露

数据丢失
系统破坏



成为“肉机”
成为跳板

木马特点

木马与病毒区别

	木马	病毒
传染性	无	有
破坏性	本身不带	本身具有
目的	非授权访问	破坏程序或系统

03

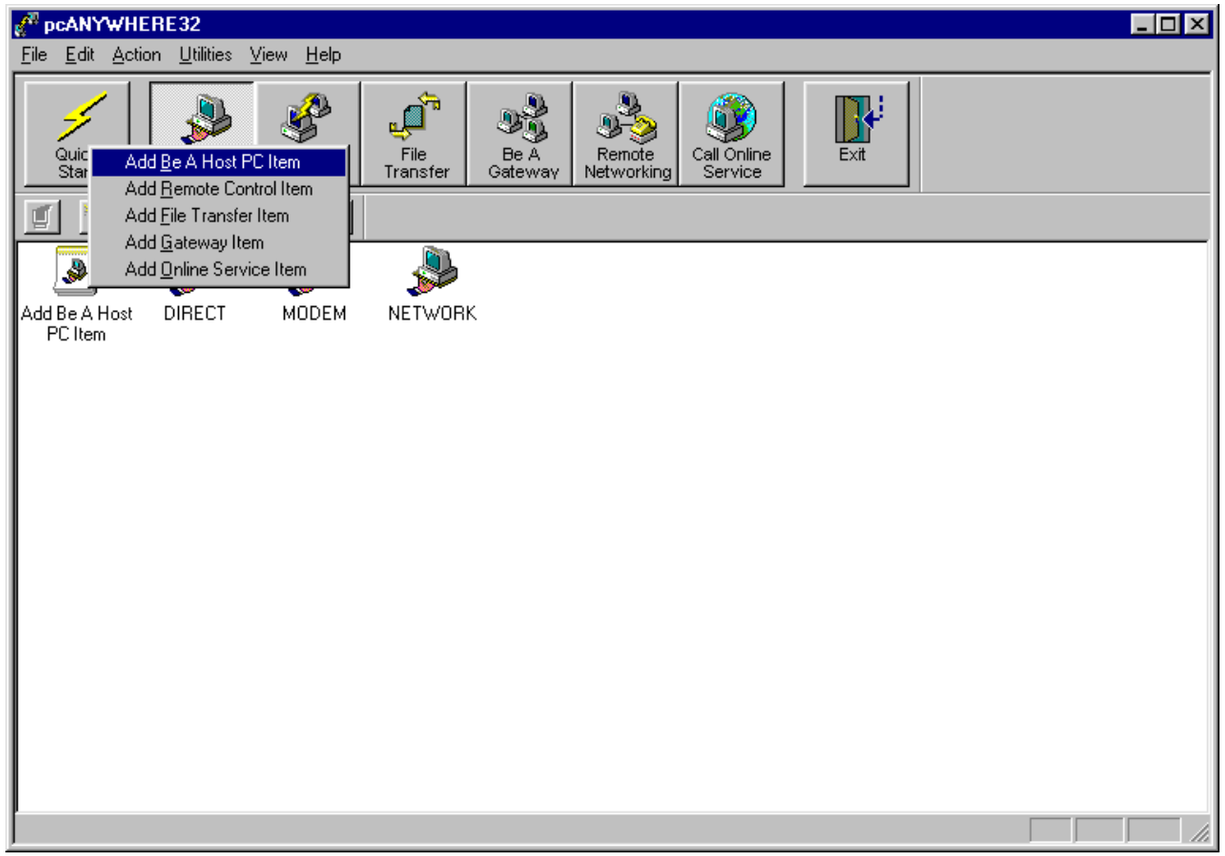
章节

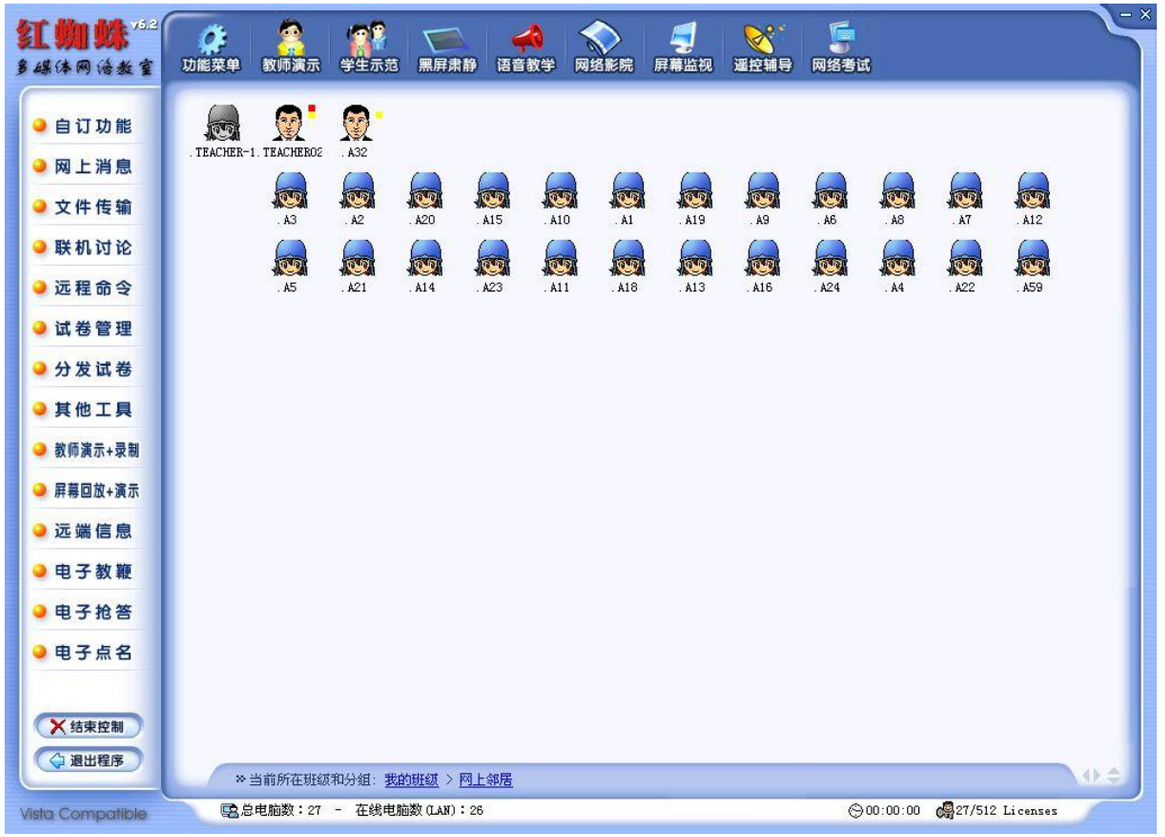
PART

木马种类

木马种类

远程访问型木马





木马种类

键盘记录型

木马种类

密码发送型


国家计算机病毒中心发现盗号木马新变种
专门窃取聊天工具账号和密码
假冒正常的屏幕保护程序文件(扩展名.scr)
实际上是一个可执行文件
采用图片图标，诱骗计算机用户点击运行
运行后
会释放并打开图片文件，同时释放一组恶意程序文件到操作系统中，并强行关闭正在运行的聊天工具应用程序进程文件
如果用户再次运行登录聊天工具账户
会导致其账户密码被盗取，并自动发送至恶意攻击者指定的网络邮件服务器上
专家建议
已感染的用户 应立即升级防病毒软件，进行全面杀毒
未感染的用户 应打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御
还要不定期地更换聊天工具的账户和密码，设置比较复杂或多位数的账户密码

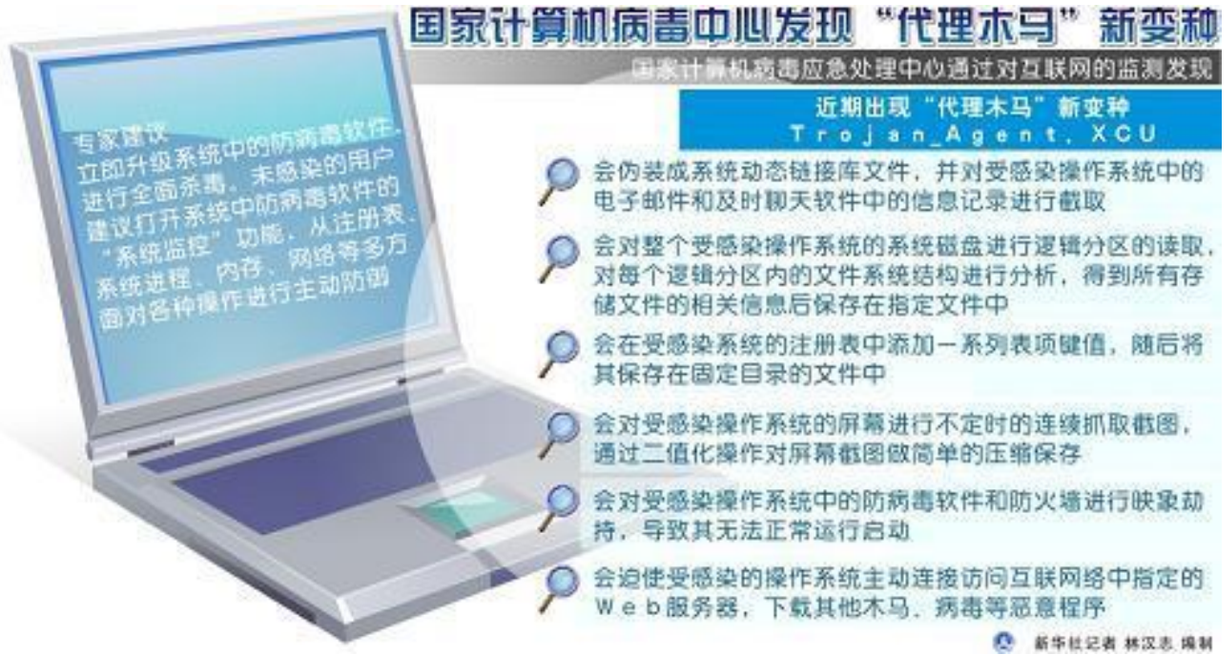
木马种类

破坏型

木马种类

代理型


嘿嘿，来钱可真快！
病毒程序
游戏账号
游戏装备


国家计算机病毒中心发现“代理木马”新变种
国家计算机病毒应急处理中心通过对互联网的监测发现
专家建议
立即升级系统中的防病毒软件，进行全面杀毒。未感染的用户建议打开系统中防病毒软件的“系统监控”功能，从注册表、系统进程、内存、网络等多方面对各种操作进行主动防御
近期出现“代理木马”新变种
Trojan_Agent.XCU
会伪装成系统动态链接库文件，并对受感染操作系统中的电子邮件和及时聊天软件中的信息记录进行截取
会对整个受感染操作系统的系统磁盘进行逻辑分区的读取，对每个逻辑分区内的文件系统结构进行分析，得到所有存储文件的相关信息后保存在指定文件中
会在受感染系统的注册表中添加一系列表项键值，随后将其保存在固定目录的文件中
会对受感染操作系统的屏幕进行不定时的连续抓取截图，通过二值化操作对屏幕截图做简单的压缩保存
会对受感染操作系统中的防病毒软件和防火墙进行映象劫持，导致其无法正常运行启动
会迫使受感染的操作系统主动连接访问互联网络中指定的Web服务器，下载其他木马、病毒等恶意程序
新华社记者 林汉志 编制

木马种类

FTP型

木马种类

下载型

04

章节

PART

木马发展

木马发展

第一代 最原始的木马程序

第二代 代表：冰河

第三代 反弹端口（灰鸽子）

木马发展

第四代 进程隐藏：广电男生

第五代 驱动级木马

第六代 黏虫技术类型和特殊反显技术类型

小结

CONTENTS

THANK YOU