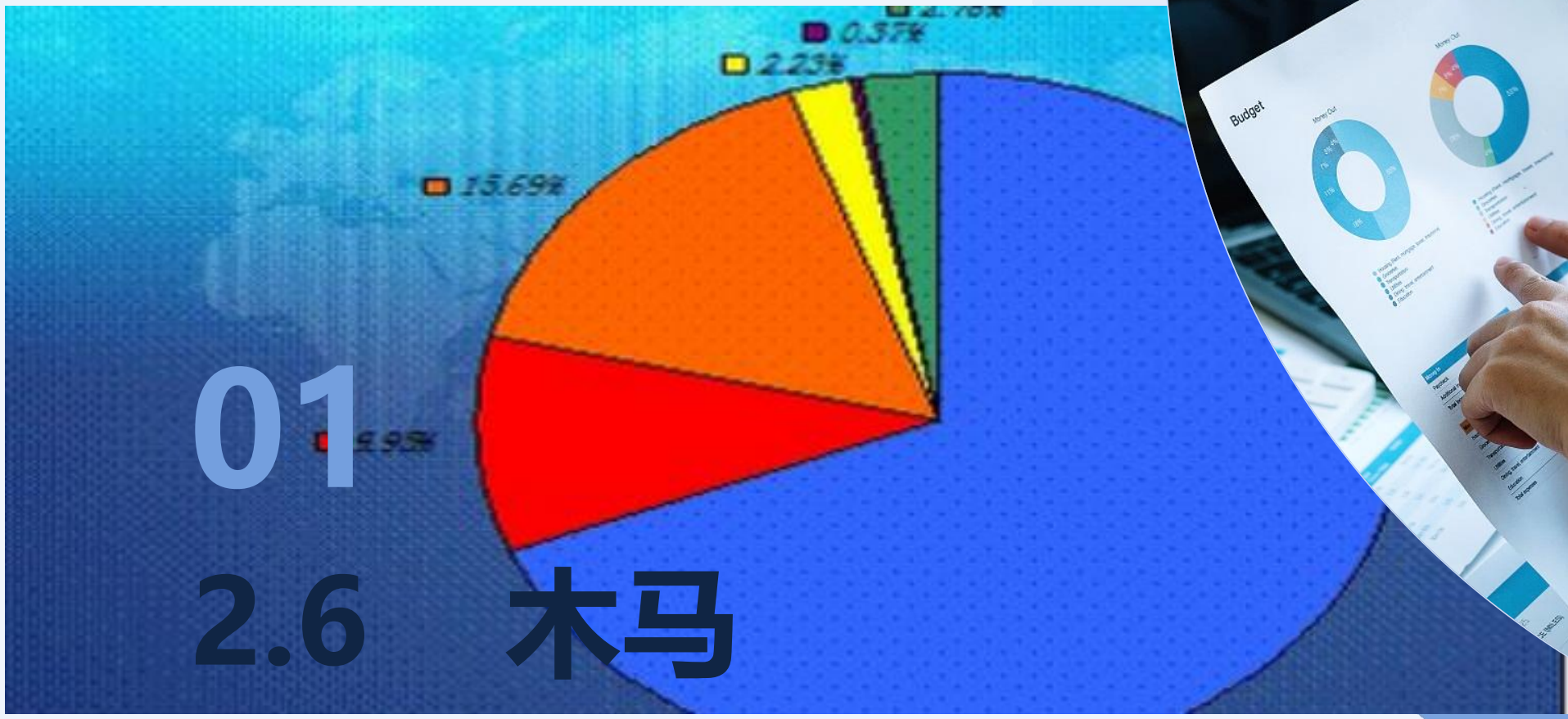
木马

木马（Trojan）木马是一种基于远程控制的黑客工具，具有隐蔽性、潜伏性、危害性 、非授权性 等典型的特征。



01

2.6 木马

主要传播的病毒类型

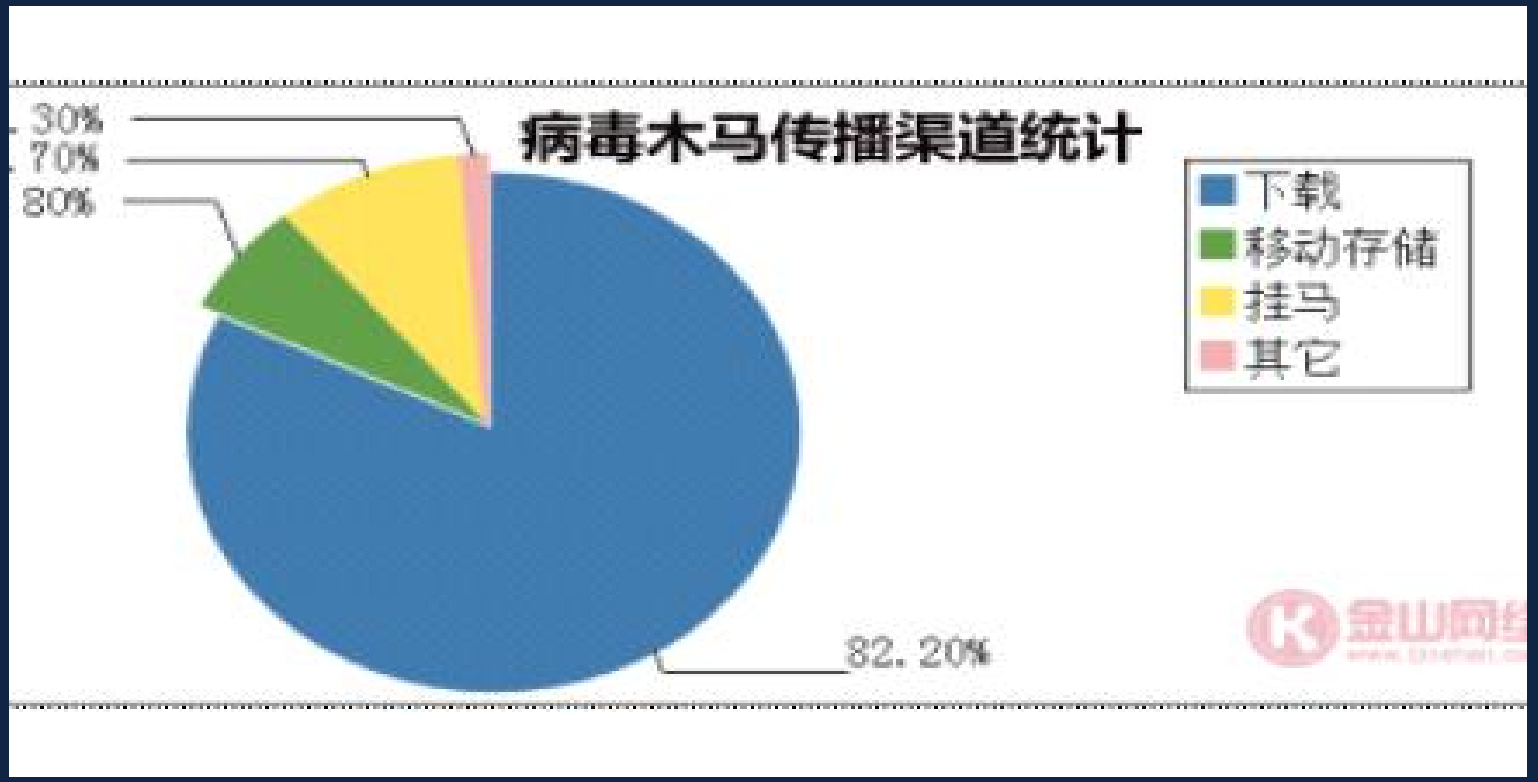
02 2.6 木马

RISING 瑞星

2019年中国网络安全报告

2019年病毒Top10

排名	病毒名	描述
1	Trojan.Vools!8.F279	利用永恒之蓝漏洞传播，攻击局域网中的计算机，传播
2	Trojan.Win32/64.XMR-Miner!1.ADCC	挖矿木马
3	Adware.AdPop!1.BA31	国内流氓软件使用的弹窗模块
4	Downloader.Adload!8.D1	下载其他广告/流氓软件的下载器木马
5	Adware.Downloader!1.B5B0	国内下载站的“高速下载器”，通常会下载流氓软件
6	Worm.VobfusEx!1.99DF	利用U盘传播的蠕虫病毒
7	Ransom.FileCryptor!8.1A7	勒索软件
8	Backdoor.Overie!1.64BD	后门程序
9	Virus.Ramnit	Ramnit感染型病毒
10	Trojan.DTLMiner	DTLMiner挖矿木马



2.6 木马

93%的木马病毒依赖互联网手段进行传播

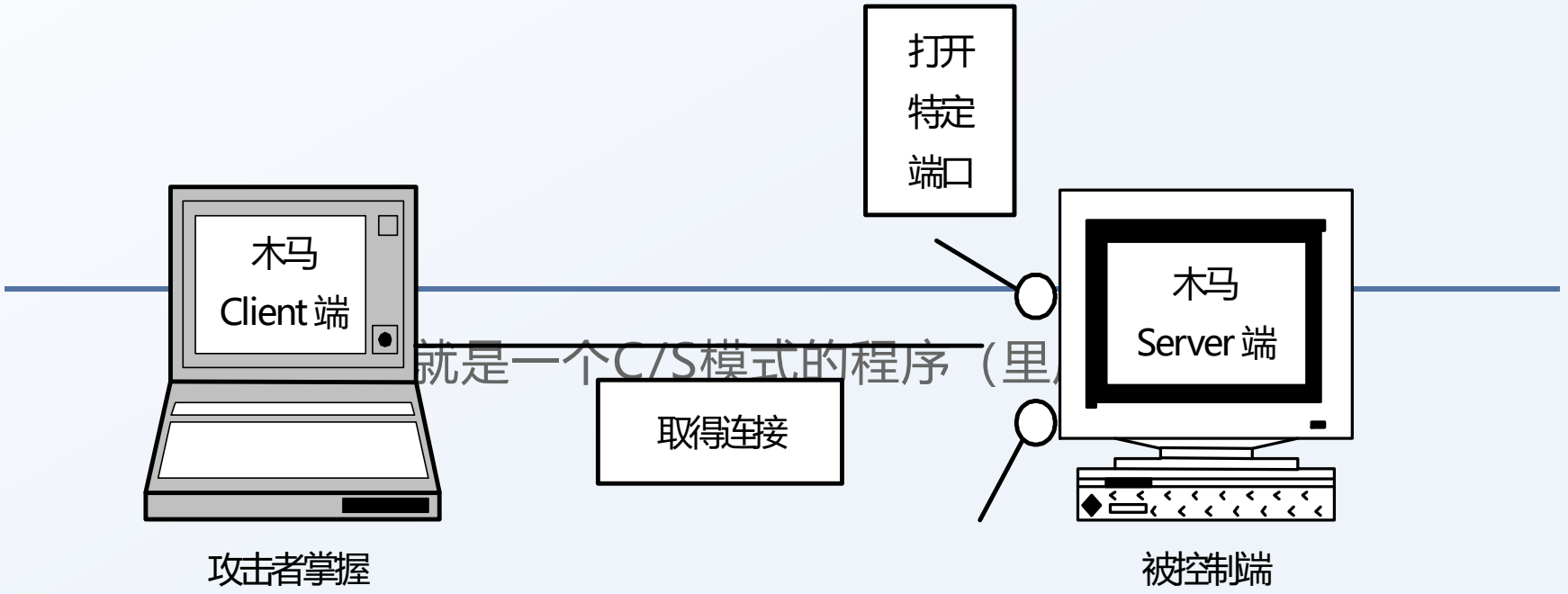
2.6.1 木马与病毒、远程控制的区别

病毒程序是以自发性的败坏为目的

木马程序是依照黑客的命令来运作，主要目的是偷取文件、机密数据、个人隐私等行为

木马和一般的远程控制软件的区别在于其隐蔽、非授权性

2.6.2 木马的工作原理



2.6.2 木马的工作原理

木马的分类


远程访问型


键盘记录型


密码发送型


破坏型


代理型


FTP型

2.6.2 木马的工作原理

木马的分类

01

传统木马

02

反弹端口木马

03

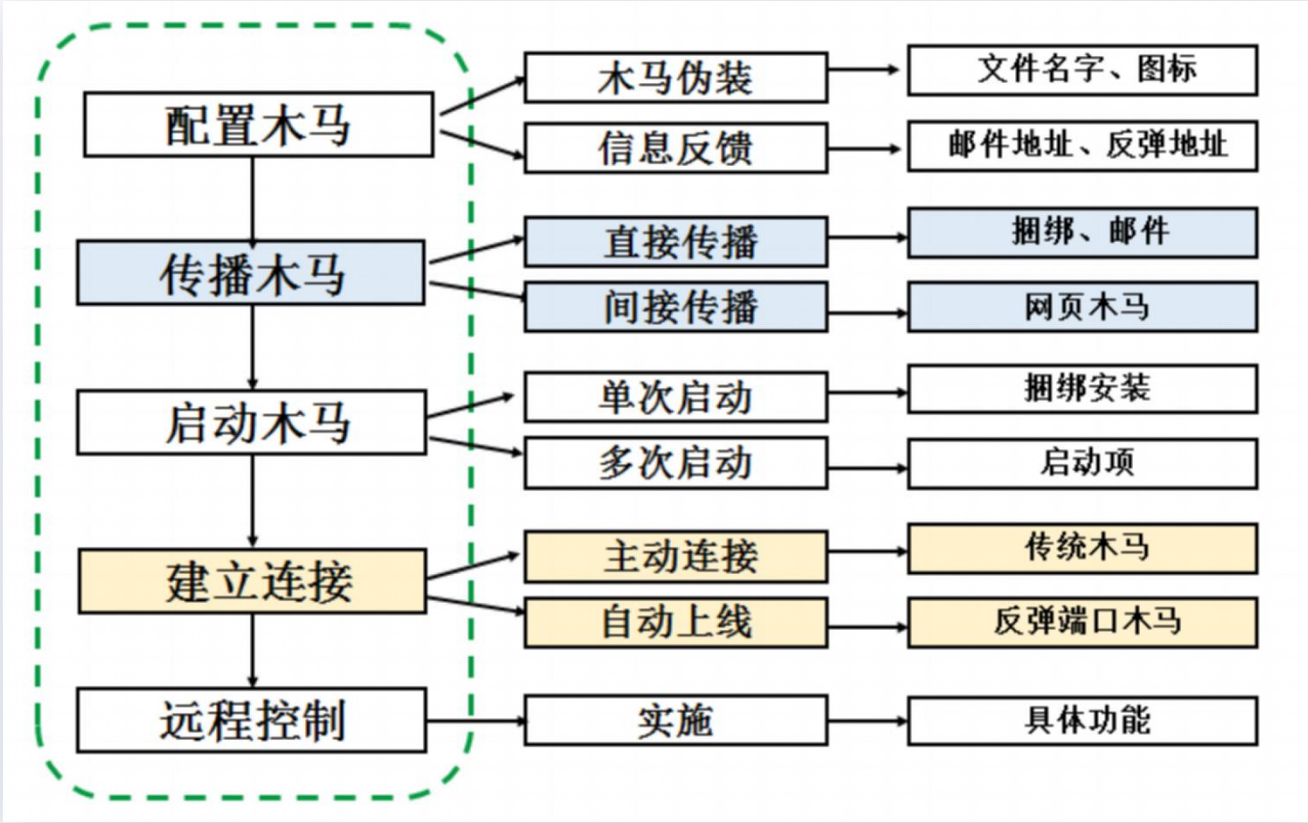
DLL木马

04

网页木马

2.6.2 木马的工作原理

木马的工作过程



2.6.2 木马的工作原理

课堂演练一：冰河木马的使用

- 服务器端程序：G-server.exe
- 客户端程序：G-client.exe
- 进行服务器配置
- 远程控制
- 如何清除?

2.6.2 木马的工作原理

反弹端口木马的工作原理

木马服务端运行后，会用邮件、ICQ 等方式发出信息通知入侵者，同时在本机打开一个网络端口监听客户端的连接。收到信息后，入侵者再运行客户端程序向服务器的这一端口提出连接请求(Connect Request)，服务器上的守护进程就会自动运行，来应答客户机的请求。

反弹端口木马的实验

目标

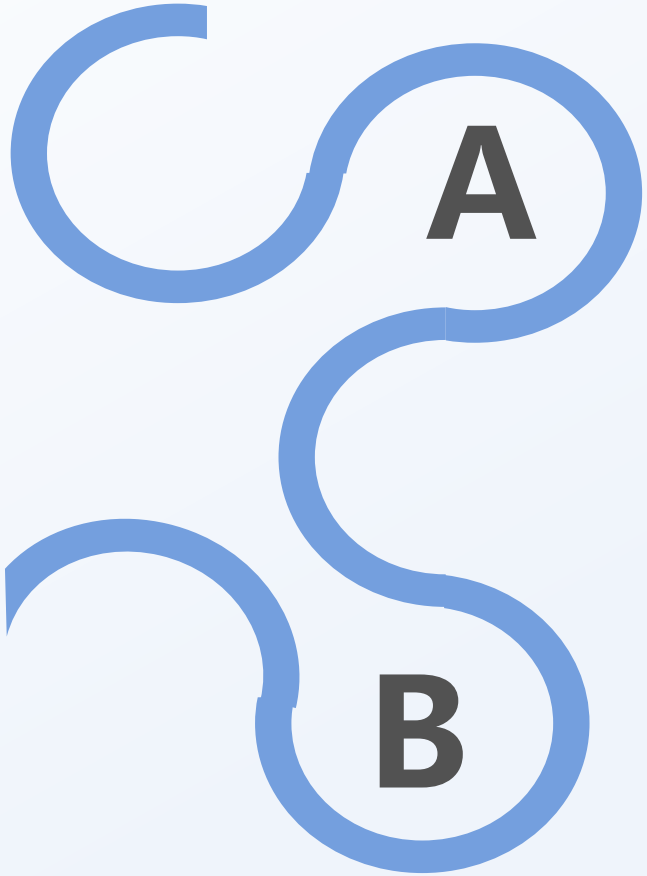
- 了解：反弹端口木马（灰鸽子）的危害；
- 熟悉：灰鸽子木马的工作原理；
- 掌握：灰鸽子木马的配置和操作；

内容

- 通过灰鸽子木马实际攻击演示操作，掌握灰鸽子木马的攻击原理，为防范灰鸽子木马的学习作准备。

2.6.2 木马的工作原理

反弹端口木马与普通木马的区别



普通木马

攻击者主动连接被攻击者

反弹端口木马

被攻击者主动连接攻击者

2.6.2 木马的工作原理

1. 木马的工作过程
2. 配置
3. 传播
4. 启动
5. 控制
6. 连接

2.6.3 DLL木马的工作原理

DLL是编译好的代码，与一般程序没什么大差别，只是它不能独立运行，需要程序调用。其实DLL的代码和其他程序几乎没什么两样，仅仅是接口和启动模式不同，DLL就变成一个独立的程序了。可以把DLL看做缺少了main入口的EXE，DLL带的各个功能函数可以看作一个程序的几个函数模块。DLL木马就是把一个实现了木马功能的代码。

特点：隐藏性（因为DLL运行时是直接挂在调用它的程序的进程里的，并不会另外产生进程。

2.6.3 DLL木马的工作原理

2.6.3 DLL木马的工作原理

木马防御