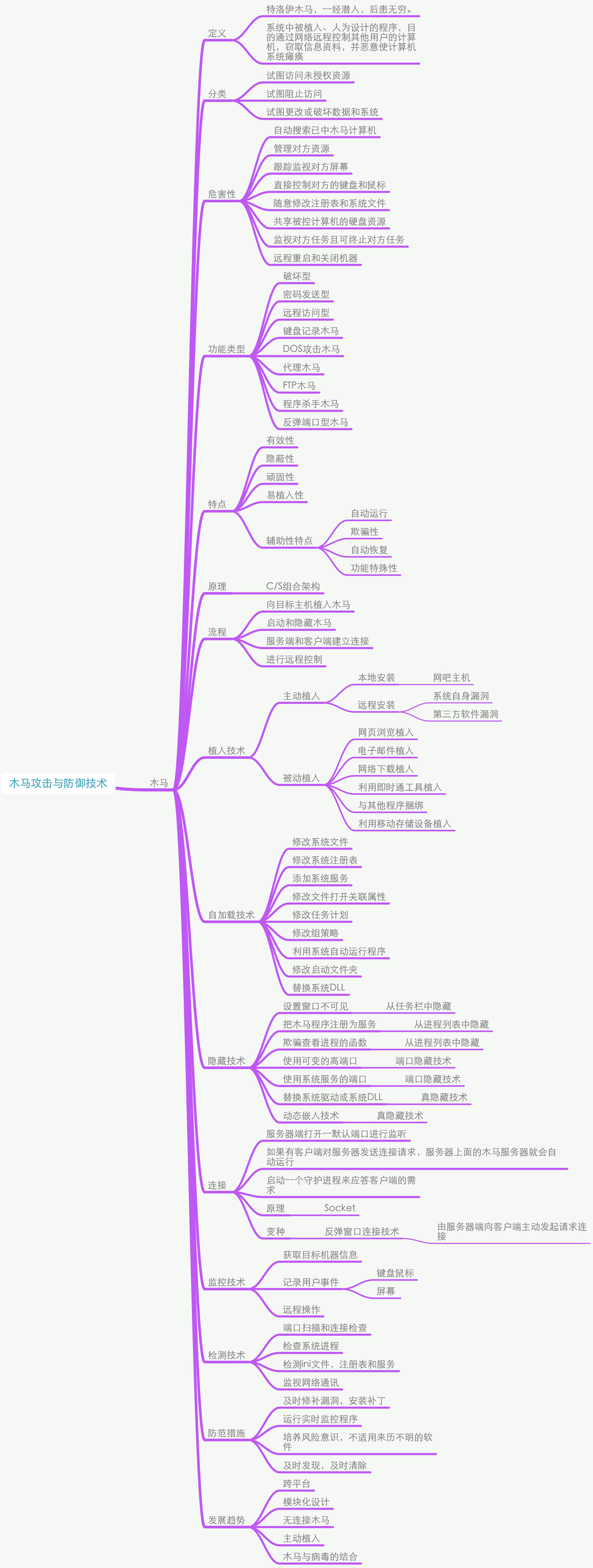
木马攻击与防御技术
木马
定义
特洛伊木马，一经潜入，后患无穷。
系统中被植入、人为设计的程序，目的通过网络远程控制其他用户的计算机，窃取信息资料，并恶意使计算机系统瘫痪
分类
试图访问未授权资源
试图阻止访问
试图更改或破坏数据和系统
危害性
自动搜索已中木马计算机
管理对方资源
跟踪监视对方屏幕
直接控制对方的键盘和鼠标
随意修改注册表和系统文件
共享被控计算机的硬盘资源
监视对方任务且可终止对方任务
远程重启和关闭机器
功能类型
破坏型
密码发送型
远程访问型
键盘记录木马
DOS攻击木马
代理木马
FTP木马
程序杀手木马
反弹端口型木马
特点
有效性
隐蔽性
顽固性
易植入性
辅助性特点
自动运行
欺骗性
自动恢复
功能特殊性
原理
C/S组合架构
流程
向目标主机植入木马
启动和隐藏木马
服务端和客户端建立连接
进行远程控制
植入技术
主动植入
本地安装
网吧主机
远程安装
系统自身漏洞
第三方软件漏洞
被动植入
网页浏览植入
电子邮件植入
网络下载植入
利用即时通工具植入
与其他程序捆绑
利用移动存储设备植入
自加载技术
修改系统文件
修改系统注册表
添加系统服务
修改文件打开关联属性
修改任务计划
修改组策略
利用系统自动运行程序
修改启动文件夹
替换系统DLL
隐藏技术
设置窗口不可见
从任务栏中隐藏
把木马程序注册为服务
从进程列表中隐藏
欺骗查看进程的函数
从进程列表中隐藏
使用可变的高端口
端口隐藏技术
使用系统服务的端口
端口隐藏技术
替换系统驱动或系统DLL
真隐藏技术
动态嵌入技术
真隐藏技术
连接
服务器端打开一默认端口进行监听
如果有客户端对服务器发送连接请求，服务器上面的木马服务器就会自动运行
启动一个守护进程来应答客户端的需求
原理
Socket
变种
反弹窗口连接技术
由服务器端向客户端主动发起请求连接
监控技术
获取目标机器信息
记录用户事件
键盘鼠标
屏幕
远程操作
检测技术
端口扫描和连接检查
检查系统进程
检测ini文件，注册表和服务
监视网络通讯
防范措施
及时修补漏洞，安装补丁
运行实时监控程序
培养风险意识，不适用来历不明的软件
及时发现，及时清除
发展趋势
跨平台
模块化设计
无连接木马
主动植入
木马与病毒的结合