YOUR LOGO

木马攻防：冰河木马案例分析

2024

主讲人：郑冬贤

时间：2024

目录

CONTENT

YOUR LOGO

Part 01

冰河木马概述

冰河木马定义

冰河木马简介

冰河木马是一款由黄鑫开发的远程控制软件，最初设计于1999年，后因功能强大被黑客用于非法入侵。

冰河木马包含控制端程序G_CLIENT.EXE和服务端程序G_SERVER.EXE，通过服务端程序控制目标主机。

冰河木马历史

01.

冰河木马的发展

冰河木马一经推出，因其强大的远程控制功能，结束了国外木马在中国市场的垄断地位，成为国产木马的代表。

冰河木马功能

冰河木马主要功能

冰河木马能够自动跟踪目标机屏幕变化、记录口令信息、获取系统信息、限制系统功能、远程文件操作、注册表操作等。

YOUR LOGO

Part 02

冰河木马攻击过程

植入冰河木马

服务端程序植入

攻击者将G_SERVER.EXE植入目标主机，该程序运行后会在目标计算机上打开7626端口，实现服务端监听。

配置服务端

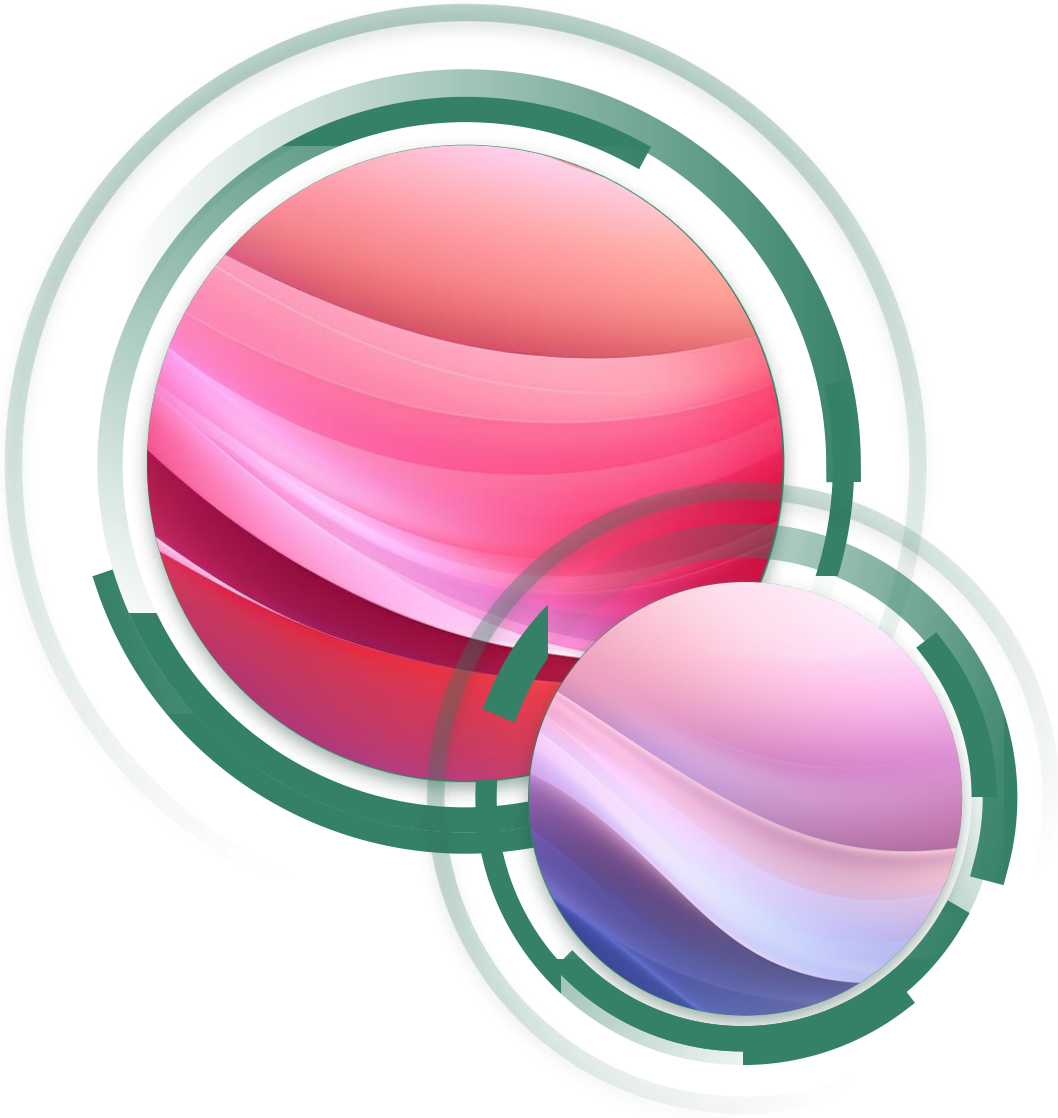
服务端配置方法

攻击者使用控制端程序G_CLIENT.EXE对木马程序进行配置，包括设置监听端口、启动方式等。

实施控制

远程控制实现

通过G_CLIENT.EXE，攻击者可以远程控制目标主机，执行文件操作、系统命令、口令记录等非法操作。



YOUR LOGO

Part 03

冰河木马防御与清除

识别木马威胁

木马威胁的发现

用户可以通过检查系统异常、注册表启动项、文件关联等方法来识别计算机是否受到冰河木马的威胁。

防御措施

防御冰河木马

用户应加强网络安全意识，定期更新系统补丁，安装杀毒软件，并避免从不可信的来源下载软件。

清除木马

手动清除方法

用户可以通过删除木马文件、清理注册表项、恢复文件关联等步骤手动清除冰河木马。

YOUR LOGO

Part 04

冰河木马的法律与伦理问题

法律问题

冰河木马的合法性

使用冰河木马进行非法入侵和远程控制是违法行为，用户应遵守法律法规，不得利用冰河木马进行非法活动。

伦理问题

冰河木马的伦理考量

冰河木马的开发和使用应遵循技术伦理，开发者和用户都应承担起保护网络安全的责任。

YOUR LOGO

谢谢大家

2024

主讲人：郑冬贤

时间：2024