南京郵電大學 Nanjing University of Posts and Telecommunications

面向COM接口的恶意代码分析技术研究

主讲人：鲁京

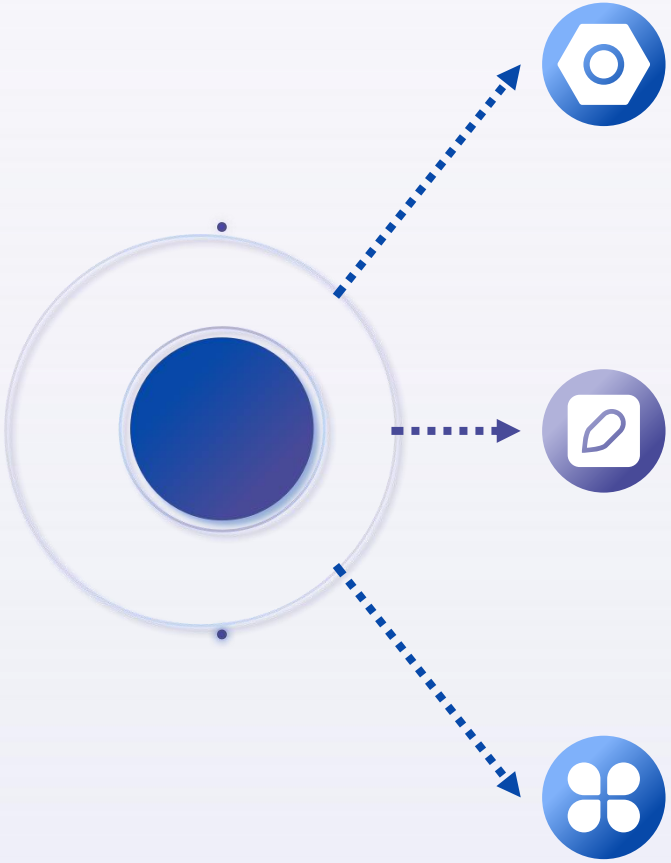
导师：沙乐天

目录

PART 01

研究背景与意义

COM技术的双刃剑特性



COM技术的广泛应用与重要性

COM（Component Object Model）是Windows系统的核心组件技术，广泛应用于ActiveX控件、OLE对象链接与嵌入、DirectX游戏引擎等，极大提升了软件的复用性。
它允许不同编程语言开发的模块进行互操作，是Windows系统的重要基石。

COM技术的恶意利用现状

恶意代码攻击者利用COM接口的隐蔽调用机制和庞杂功能，通过合法COM对象执行恶意行为，实现隐蔽后门、顽固持久化、权限提升和UAC绕过。
COM接口成为恶意代码攻击者的青睐载体，对用户和系统安全造成严重威胁。

现有检测体系的不足

COM调用复杂，与海量正常系统行为混淆，传统基于签名的检测方法难以精准识别恶意行为。
“COM恶意代码存在面广且具有较强潜伏性不易发现”是当前网络安全领域的重要痛点。

研究意义

理论研究意义

深入分析被恶意代码利用的COM接口行为，探索构建新的检测方法，填补现有检测系统对COM恶意行为分析检测的空白。

实际应用价值

为未来更智能、更准确的恶意代码检测工具研发提供技术支撑，提升网络空间安全防范能力。

对现有安全体系的补充

现有安全体系在应对COM恶意代码方面存在不足，本研究方法可作为补充，增强整体安全防护能力。