

安全技术

## Windows Rootkit进程隐藏与检测技术

王雷, 凌翔

(电子科技大学通信抗干扰技术国家级重点实验室, 成都 610054)

收稿日期 修回日期 网络版发布日期 接受日期

**摘要** 进程隐藏是Rootkit技术的一种典型应用, 隐藏运行的恶意代码威胁到计算机的安全。为此, 通过分析Windows系统中利用Rootkit技术对进程进行隐藏的原理, 针对用户模式和内核模式2种模式下进程隐藏技术的特点, 提出几种不依赖于系统服务的隐藏进程检测技术。此类检测方法直接利用系统底层的数据结构, 检测能力强。

**关键词** [Rootkit技术](#); [进程隐藏](#); [进程检测](#); [系统内核](#)

**分类号** [TP316](#)

**DOI:**

通讯作者:

作者个人主页: 王雷;凌翔

### 扩展功能

本文信息

- ▶ [Supporting info](#)
- ▶ [PDF \(299KB\)](#)
- ▶ [\[HTML全文\]\(0KB\)](#)
- ▶ [参考文献\[PDF\]](#)
- ▶ [参考文献](#)

服务与反馈

- ▶ [把本文推荐给朋友](#)
- ▶ [加入我的书架](#)
- ▶ [加入引用管理器](#)
- ▶ [引用本文](#)
- ▶ [Email Alert](#)
- ▶ [文章反馈](#)
- ▶ [浏览反馈信息](#)

相关信息

- ▶ [本刊中包含“Rootkit技术; 进程隐藏; 进程检测; 系统内核”的相关文章](#)
- ▶ [本文作者相关文章](#)