计算机应用 2006 26 (09): 2134-2136 ISSN: 1001-9081 CN: 51-1307/TP

信息安全

利用核心态钩挂技术防止代码注入攻击

朱若磊[1,2]

广东商学院信息学院[1]

收稿日期 2006-3-16 修回日期 网络版发布日期 2006-8-31 接受日期

摘要 为防止代码注入攻击，利用钩挂技术来监视有关的API函数调用十分必要。由于Windows NT系统中存在着严格的进程隔离机制，此种钩挂要在核心态下才有效。提出并讨论了实现此种技术的一种简便的方法。实践表明，在Windows XP系统条件下，利用它能够成功阻止木马利用代码注入实现攻击。

Abstract To prevent code injection attack, it is necessary to monitor involved API(Application Programming Interface) by hooking them. Because there exists rigid process isolation in Windows NT, hooking these APIs must be done in kernel mode. A relatively simple way to do this was introduced. It is proved that in Windows XP the way to hook API in kernel mode can efficiently prevent code injection attack.

关键词 代码注入 钩挂 核心态

Key words ;Code injection;hook;kernel mode

分类号

DOI:

通讯作者:
朱若磊 hg-hgzzz@sohu.com;hg-hgzzz@hotmail.com

作者个人主页: 朱若磊