[网络安全自学篇] 九十二.《Windows黑客编程技术详解》之病毒启动技术创建进程API、突破SESSION0隔离、内存加载详解（3）

原创

Eastmount 于 2020-07-27 17:41:49 发布 10799 收藏 108

分类专栏： 网络安全自学篇 文章标签： Windows黑客编程 启动技术 病毒分析 内存加载 安全攻防

这是作者网络安全自学教程系列，主要是关于安全工具和实践操作的在线笔记，特分享出来与博友们学习，希望您喜欢，一起进步。这篇文章将带着大家来学习《Windows黑客编程技术详解》，其作者是甘迪文老师，推荐大家购买来学习。作者将采用实际编程和图文结合的方式进行分享，并且会进一步补充知识点。第三篇文章主要介绍木马病毒启动技术，包括创建进程API、突破SESSION0隔离、内存加载详解，希望对您有所帮助。

病毒木马植入模块成功植入用户计算机后，便会开启攻击模块来对用户计算机数据实施窃取和回传等操作。通常植入和攻击是分开在不同模块之中的，这里的模块指的是DLL、exe或其他加密的PE文件等。只有当前植入模块成功执行后，方可继续执行攻击模块，同时会删除植入模块的数据和文件。

模块化开发的好处不单单是便于开发管理，同时也可以减小因某一模块的失败而导致整个程序暴露的可能性。本文重点介绍病毒木马启动技术，包括：

- 创建进程API：介绍使用WinExec、ShellExecute以及CreateProcess创建进程
- 突破SESSION 0隔离创建进程：主要通过CreateProcessAsUser函数实现用户进程创建
- 内存直接加载运行：模拟PE加载器，直接将DLL和exe等PE文件加载到内存并启动运行