[网络安全自学篇] 九十三.《Windows黑客编程技术详解》之木马开机自启动技术（注册表、计划任务、系统服务）

原创

Eastmount 于 2020-08-15 19:28:15 发布 11970 收藏 169

分类专栏： 网络安全自学篇 文章标签： 自启动 病毒分析 Windows黑客编程 注册表启动 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。第四篇文章主要介绍木马病毒自启动技术，包括注册表、快速启动目录、计划任务和系统服务，希望对您有所帮助。

对于一个病毒木马来说，重要的不仅是如何进行破坏，还有如何执行。同样，如何开始也非常重要，病毒木马只有加载到内存中开始运行，才能真正体现出它的破坏力。否则，它只是一个普通的磁盘文件，对于计算机用户的数据、隐私构不成任何威胁。

即使成功植入模块并启动攻击模块，依然不能解决永生驻留的问题（持久性攻击）。解决永生驻留的第一步便是如何实现伴随系统启动而启动的问题，即**开机自启动**。这样，即使用户关机重启，病毒木马也随着系统的启动，而由系统加载到内存中运行，从而窃取用户数据和隐私。因此，开机自启动技术是病毒木马至关重要的技术，也是杀软重点监测的技术。对于杀软来说，只要把守住自启动的入口，就可以把病毒木马扼杀在摇篮中。