[网络安全自学篇] 八十七.恶意代码检测技术详解及总结

原创

Eastmount 于 2020-07-16 12:03:44 发布 19059 收藏 226

分类专栏： 网络安全自学篇 文章标签： 网络安全 恶意代码 检测技术 系统安全 安全防御

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。前文分享了威胁情报分析，通过Python抓取FreeBuf网站“APT”主题的相关文章。这篇文章将详细总结恶意代码检测技术，包括恶意代码检测的对象和策略、特征值检测技术、校验和检测技术、启发式扫描技术、虚拟机检测技术和主动防御技术。基础性文章，希望对您有所帮助~

自全球第一个计算机病毒出现后，人们通过与病毒长期的斗争，积累了大量反病毒经验，掌握了大量实用的反病毒技术，并研制出一系列优秀的反病毒产品，主要用于病毒的防护、检测及其清除等。病毒的检测技术主要包括特征值检测技术、校验和检测技术、启发式扫描技术、虚拟机检测技术、主动防御技术，以及新兴的云查杀技术等。个人用户也可以通过经验、安全检测工具和反病毒软件来检查计算机是否感染病毒，或是采用沙箱及相关静、动态分析手段来对病毒进行深入分析。

作者作为网络安全的小白，分享一些自学基础教程给大家，主要是关于安全工具和实践操作的在线笔记，希望您们喜欢。同时，更希望您能与我一起操作和进步，后续将深入学习网络安全和系统安全知识并分享相关实验。总之，希望该系列文章对博友有所帮助，写文不易，大神们不喜勿喷，谢谢！如果文章对您有帮助，将是我创作的最大动力，点赞、评论、私聊均可，一起加油喔~

文章目录