[网络安全自学篇] 八十九.PE文件解析之通过Python获取时间戳判断软件来源地区

原创

Eastmount 于 2020-07-23 15:05:40 发布 8361 收藏 37

分类专栏： 网络安全自学篇 文章标签： 软件安全 溯源 PE文件 Python 地区分析

本文链接：https://blog.csdn.net/Eastmount/article/details/107384250

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。前文分享了基于机器学习的恶意代码检测技术，包括机器学习概述与算法举例、基于机器学习方法的恶意代码检测、机器学习算法在工业界的应用。这篇文章将尝试软件来源分析，结合APT攻击中常见的判断方法，利用Python调用扩展包进行溯源，但也存在局限性。文章同时也普及了PE文件分析和APT溯源相关基础，基础性文章，希望对您有所帮助~

你是否想过如何判断PE软件或APP来源哪个国家或地区呢？你又想过印度是如何确保一键正确卸载中国APP呢？使用黑白名单吗？本文尝试进行软件来源溯源，目前想到的方法包括：

- 通过PE文件分析抓取创建文件时间戳，然后UTC定位国家地区，但受样本数量较少，活动规律不稳定影响很大
- 通过静态分析获取非英文字符串，软件中一般有供该国使用的文字，然后进行编码比对溯源地区
- 某些APP或软件存在流量反馈或IP定位，尝试进行流量抓取分析
- 利用深度学习进行分类，然后提取不同国家的特征完成溯源

欢迎大家讨论和留言，我们一起进行更深入的尝试和安全测试 O(∩_∩)O

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、