

[网络安全自学篇] 十.论文之基于机器学习算法的主机恶意代码

原创

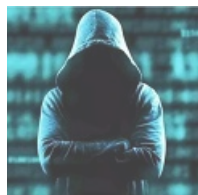
[Eastmount](#) 于 2019-09-15 21:55:15 发布 11692 收藏 80

分类专栏: [网络安全自学篇](#) 文章标签: [网络安全](#) [恶意代码](#) [机器学习](#) [论文普及](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/Eastmount/article/details/100784947>

版权



[网络安全自学篇](#) 专栏收录该内容

107 篇文章 2590 订阅 ¥19.90 ¥99.00

订阅专栏

这是作者的系列网络安全自学教程, 主要是关于网安工具和实践操作的在线笔记, 特分享出来与博友共勉, 希望您们喜欢, 一起进步。前文分享了Web漏洞及端口扫描之Nmap、ThreatScan和DirBuster工具, 社会工程学中的IP物理位置定位、IP获取、手机和邮箱查找、文件属性等。本篇文章, 作者将分享两篇论文, 机器学习是如何运用到恶意代码攻击中的, 并谈谈自己的理解, 后续深入研究尝试分享相关实验, 目前还是小白一只。基础性文章, 希望对初学者有帮助, 大神请飘过, 谢谢各位看官!

百度网盘: https://pan.baidu.com/s/1dsunH8EmOB_tIHXXguOeA 提取码: izeb

参考文献:

- [1] 张东, 张尧, 刘刚, 宋桂香. 基于机器学习算法的主机恶意代码检测技术研究[J]. 网络与信息安全学报, 2017(7): 25-32.
- [2] 杨轶, 苏璞睿, 应凌云, 等. 基于行为依赖特征的恶意代码相似性比较方法[J]. 软件学报, 2011, 22(10): 2438-2453.
- [3] 杨晔. 基于行为的恶意代码检测方法研究[D]. 西安: 西安电子科技大学, 2015.
- [4] 李盼, 赵文涛, 刘强+, 崔建京, 殷建平. 机器学习安全性问题及其防御技术研究综述, 计算机科学与探索, 2018(12).
- [5] 张蕾, 崔勇, 刘静, 江勇, 吴建平. 机器学习在网络空间安全研究中的应用[J]. 计算机学报, 2018(9): 1943-1975.
- [6] IMRAN M, AFZAL M T, QADIR M A. Malware classification usi