

# [网络安全自学篇] 七十四.APT攻击检测溯源与常见APT组织的攻击案例

原创

Eastmount 于 2020-05-11 18:10:35 发布 15818 收藏 84

分类专栏: [网络安全自学篇](#) [APT分析及溯源](#) 文章标签: [网络安全](#) [APT攻击](#) [案例分析](#) [溯源](#) [系统安全](#)

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/106009460>

版权



[网络安全自学篇](#) 同时被 2 个专栏收录

107 篇文章 2590 订阅 ¥19.90 ¥99.00

订阅专栏



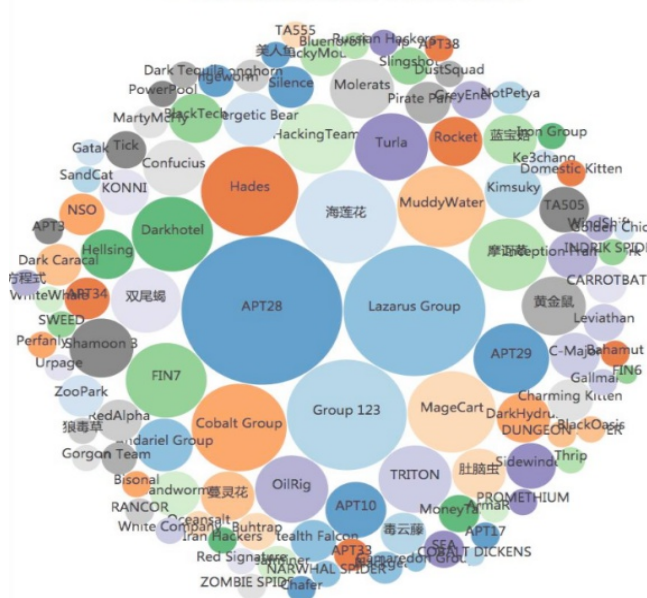
[APT分析及溯源](#)

15 篇文章 49 订阅

订阅专栏

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WannaCry蠕虫的传播机制, 带领大家详细阅读源代码。这篇文章将分享APT攻击检测溯源与常见APT组织的攻击案例, 并介绍防御措施。希望文章对您有所帮助~

2018年公开披露的高级威胁类攻击组织和行动



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

一.什么是APT攻击

二.常见APT组织的攻击案例

1.海莲花（APT32）

2.摩诃草（APT-C-09）

3.蓝宝菇（APT-C-12）

4.SideWinder（T-APT-04）

<