实验一：APT 分析报告所使用的溯源技术调研与实践

一．目标

- 了解并实战常见 APT 事件的分析思路与报告框架
- 结合课堂所学，调研和体验安全厂商使用的溯源方法

二．要求

- 自由组队，6 人 1 组；
- 从相关材料中或其它来源挑选含有溯源分析内容的报告，建议选取一个系列，如针对同一个攻击者/攻击组织，或针对某一系列攻击活动所进行的追踪溯源报告；
- 总结其使用的溯源方法——包括但不限于溯源的技术（与课堂内容相结合，对应到溯源的 4 个层次，注意提供分析流程等图表），溯源结果——包括但不限于体现归因的信息、攻击活动序列、攻击者/攻击组织画像，并评价该方法的优劣与溯源结果的可信度，形成相应的调研报告；
- 在可控环境进行了重现式验证并在报告中体现，可加分；
- 不得写成样本分析报告。

三．相关材料

- 部分 APT 分析报告汇总地址：

  https://github.com/CyberMonitor/APT_CyberCriminal_Campagin_Collections

四．交付物与截止时间

- 覆盖溯源方法、溯源结果、方法与效果评价等核心内容的课堂讲解展示（10~15 分钟），在 10 月 25 日的“经典 APT 分析报告使用的溯源技术研讨”上讲述。**PPT 在 11 月 8 日前加密（密码约定 syqz2018!），发到邮箱 yao_ye_peng@163.com。**
- 符合前述“要求”的 word 版调研分析报告在 11 月 8 号前与上述 PPT 及相关样本文件打包，按“溯源取证课-系列或主题名称-组长学号-组长姓名-溯源调研”形式命名，加密发送到邮箱 **yao_ye_peng@163.com。**
- 注意列出原始文献。
- 不得直接拷贝粘贴图表，图表不得有水印。
- Word 版报告篇幅不宜少于 8000 字。
- 注意**体现成员的分工/贡献。**

五．部分系列参考

- Patchwork/APT-C-09/Victory Tiger/摩诃草/白象/ Dropping Elephant/Hangover/MONSOON/Operation Hangover
- Unit 8200/ Equation Group/Tilded Team/ Longhorn：可加分
- APT28/Sednit/Sofacy/Pawn Storm/Fancy Bear/STRONTIUM/Tsar Team/Threat Group-4127
- APT29/The Dukes/Cozy Bear/CozyDuke
- APT32/OceanLotus Group
- APT37/ScarCruft/Reaper/Group123/TEMP.Reaper

- Cleaver/TG-2889/Threat Group 2889
- Lazarus Group/HIDDEN COBRA/Guardians of Peace/ZINC/NICKEL ACADEMY
- Magic Hound/Rocket Kitten/Operation Saffron Rose/Ajax Security Team/Operation Woolen-Goldfish/Newscaster/Cobalt Gypsy
- Turla/Waterbug/WhiteBear
- Etc…

注：**各组所选系列不要重复**

各组组长尽快将所选系列与成员组成发给助教姚叶鹏，先选先得。