上海交通大学
SHANGHAI JIAO TONG UNIVERSITY

2022 数据可视化竞赛
ChinaVis DataChallenge

黑灰产网络资产图谱可视化分析

林宇欣，王祎雯，胡杰民，胡屹垚
指导老师：董笑菊

选题背景

在当前互联网生态中，存在有大量利用信息技术和网络技术，实施各类违法犯罪活动，以此谋取不正当利益的网络黑灰产业。这样的存在将会威胁到网络生态的健康发展，侵犯网民的合法权益，需要予以严厉打击。

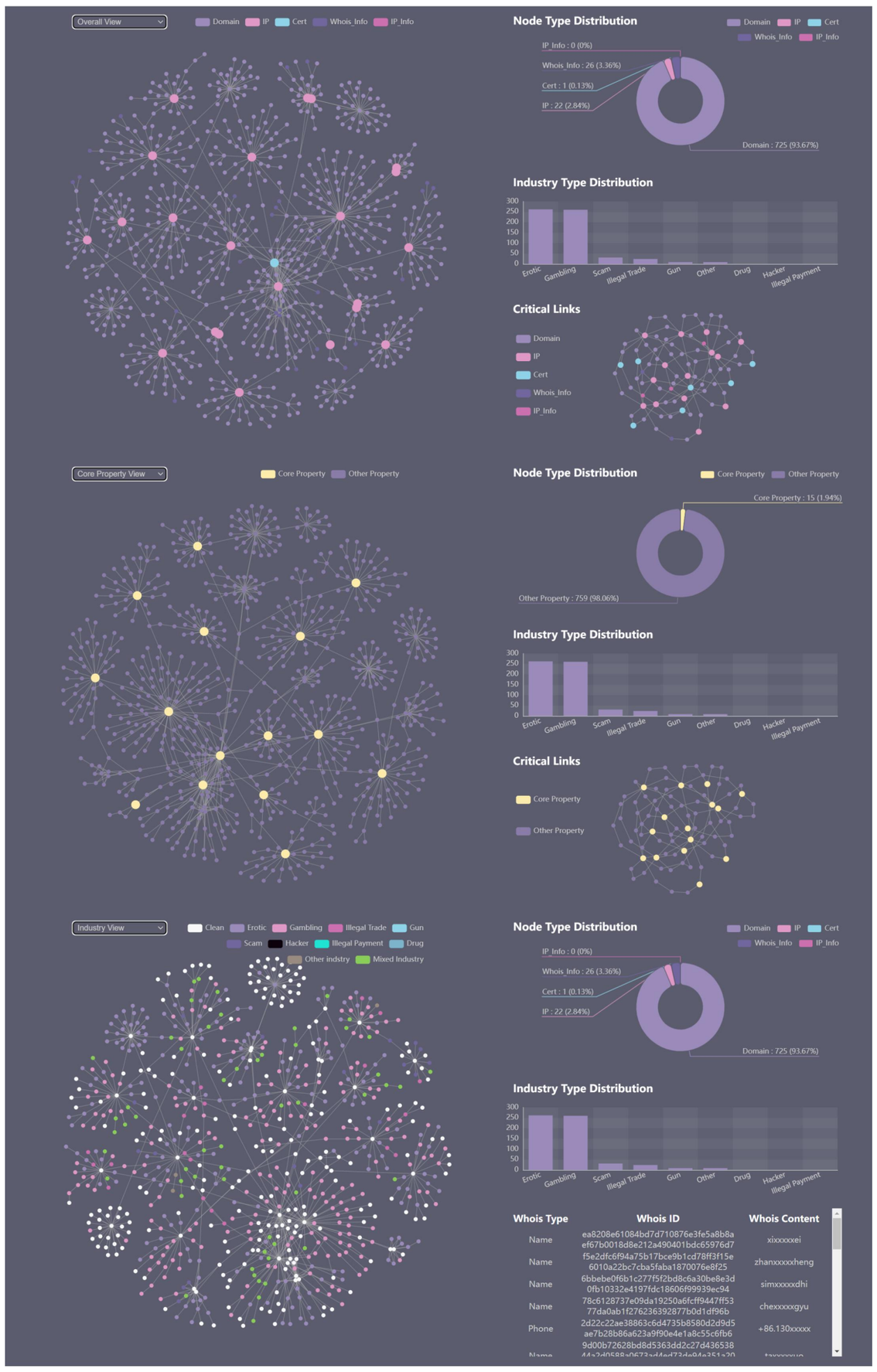
考虑到网络黑灰产业链条化、团伙化、资产化和跨域化的特点，我们认为查证和封堵黑灰产团伙的核心资产站点是打击黑灰产团伙的重要切入点。基于上述原因，我们决定给出一套可视化方案，识别黑灰产团伙的网络资产子图，推断其中的关键链路和核心资产节点，并以此为依据分析每个黑灰产团伙网络运作机制，以供网络黑灰产治理人员参考。

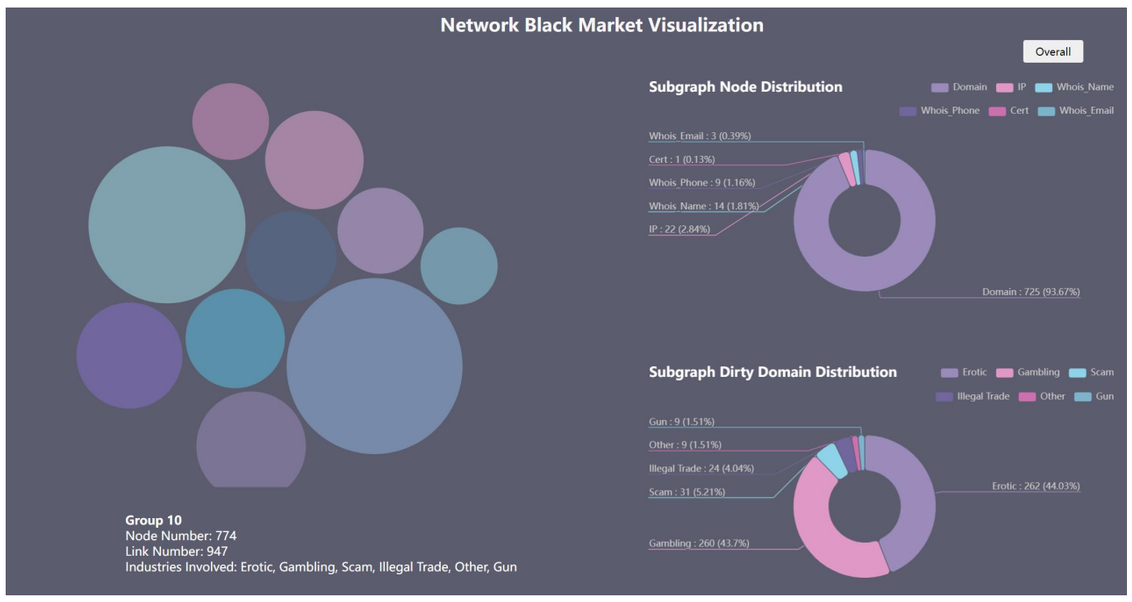
解决方案

对于已知线索节点的黑灰产团伙，我们采用多起点的广度优先遍历算法挖掘其网络资产子图，并删除孤点维护子图的连通性。随后，通过图数据库工具Neo4j对不同结构的黑产网络建模，我们也筛选出了此外的数个潜在的黑灰产团伙。我们采用Echarts的力导向图可视化了上述资产子图，并对节点类别，涉黑灰产类别等信息分别予以了统计。

我们基于黑灰产网络子图核心资产和关键链路识别规则，给出了每个黑灰产团伙的核心节点与关键链路，并采用可视化的方式展示了相应结构。针对每个团伙，我们提供了网络域名注册人的信息列表，以供索引团伙的相关负责人。

可视化系统总览





如上图所示，在我们的可视化系统主界面中，给出了与规模呈正相关的黑灰产团伙气泡图，并在下方注明了相应团伙的基本信息。我们在界面右侧提供了黑灰产网络节点类别和资产分布的整体统计信息，以及每个团伙的资产子图统计信息。

点击指定团伙对应的气泡，将会进入详细的网络资产子图界面。以其中一个潜在黑灰产团伙为例，左图为包括总览界面、关键资产分布界面和黑灰产分布界面在内的团伙三视界面。界面左侧给出了网络资产子图的力导向图，并分别根据节点类别、核心资产和涉黑灰产业类别进行了着色；界面右侧给出了相关分类的统计信息，以饼图和自动降序柱状图的方式予以展示。此外，界面右下方提供了子图与左侧力引导图以相同方式着色的关键链路和涉黑灰产业的网络域名注册人详细信息。三视界面采用左上方的下拉框进行切换。

左图中的黑灰产团伙是一个中大型团伙，包含774个节点和947条连边，其中大部分节点均与非法活动直接相关。该团伙主营赌博与色情业务，也有少量子团伙进行诈骗和非法交易。根据域名注册人推断，其主要负责人共有14人次，以xixxxxxei和zhanxxxxxheng为团伙核心。团伙内部采用了大量域名跳板，并最终汇聚在同一个证书节点上。对该证书节点和其他相关关键资产进行查封，可以对该黑灰产团伙造成难以恢复的严重打击。

项目总结

基于相关挖掘算法，我们找出了给出线索的5个黑灰产团伙，并另外挖掘出了5个潜在的黑灰产团伙。利用我们的可视化系统，我们识别出了每个团伙的关键链路和核心节点，了解了团伙的主营黑灰产业务，并以子图的结构作为依据，分析了相关团伙的运作机制，找出了可供追责的团伙负责人和应当被打击的团伙核心资产。