

黑灰产网络资产图谱可视化

程序设计思想与方法大作业

Log Creative

2022 年 5 月 9 日

背景

本项目使用黑灰产网络数据集，可视化其黑灰产核心资产之间的联系有助于侦查人员破获相关案件。`Node.csv` 中含有黑灰产网络中的节点，`Link.csv` 中含有该网络中节点的连接信息。

设计思想

采用统一代价搜索（UCS）算法（实现于 `ucs.py` 中）从线索节点出发，对网络进行挖掘。之后对于任意一个核心节点，也可以获得从该核心节点出发到其他核心节点的关键路径。由于两种功能的算法相同，故采用同一个 UCS 父类进行算法设计，采用 `searchUCS` 和 `pathUCS` 子类对接口进行实现。

挖掘遵循一定的规则，最重要的限制是从起始线索节点出发不能挖掘超过 3 跳的节点，相同的邻居节点类型将会只取前 20 个用于访问，以及该子图的规模（节点数、边数）根据设置的 `Limitation` 不同而被限制。

最后采用 `tkinter` 对节点进行步进可视化，按照矩阵的样式在 `Canvas` 中展示图形。使用了下拉选单、按钮等 `tkinter` 内置控件。

功能

1. 选择线索节点按照限制要求对图进行挖掘，找到关键节点。
2. 选择一个核心节点，获取到达其他核心节点的所有关键路径。
3. 再选择一个核心节点，可以得到两个节点间的关键路径。

使用方法

命令行中运行（需要使用 Python 3）

```
python main.py
```

等待数据加载完成后，即可看到图形界面。

tk

Node ID: Node

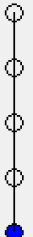
Limitation: Edge

选择起始节点与限制之后，按下 **Generate** 开始生成。

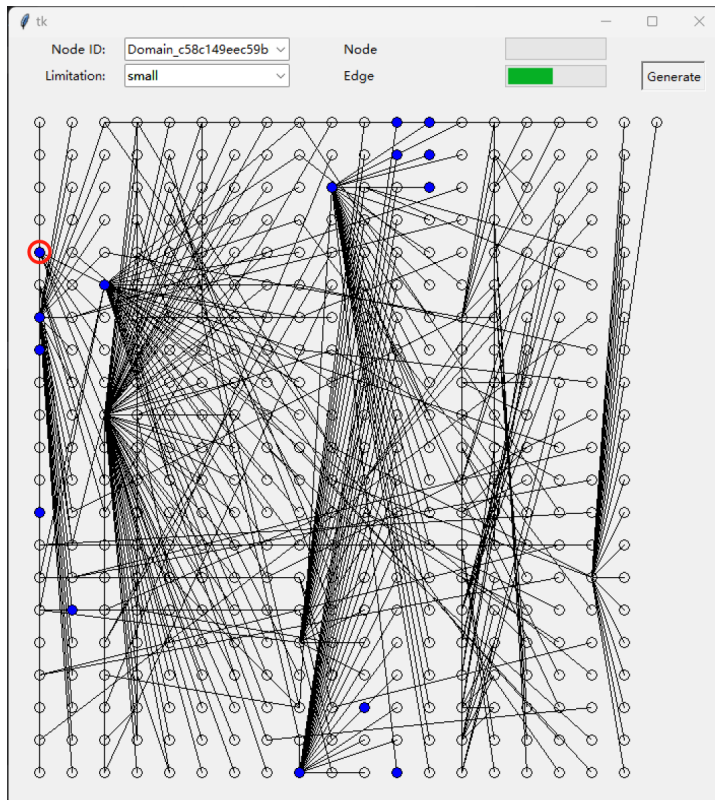
tk

Node ID: Domain_1d8e02f35e2cbz

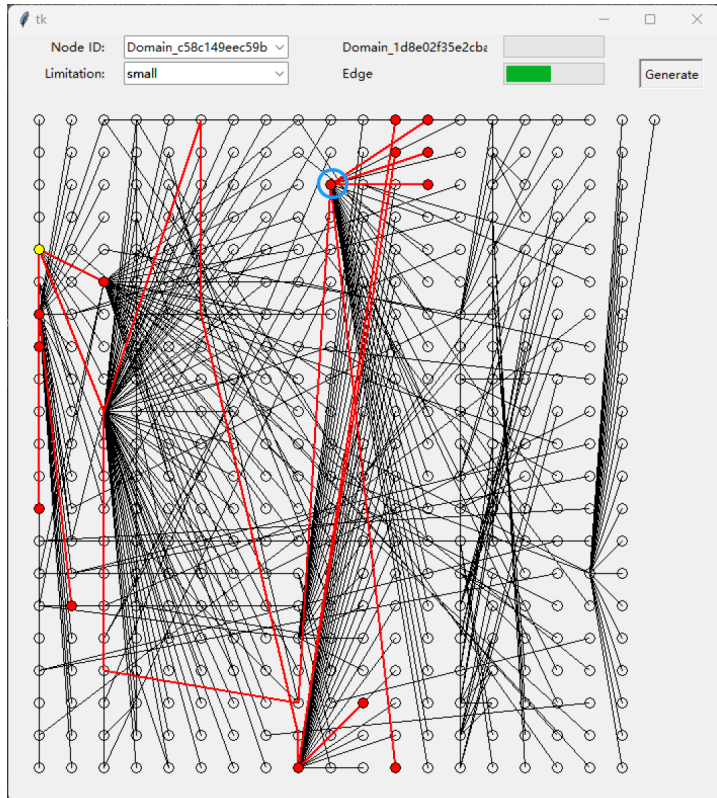
Limitation:



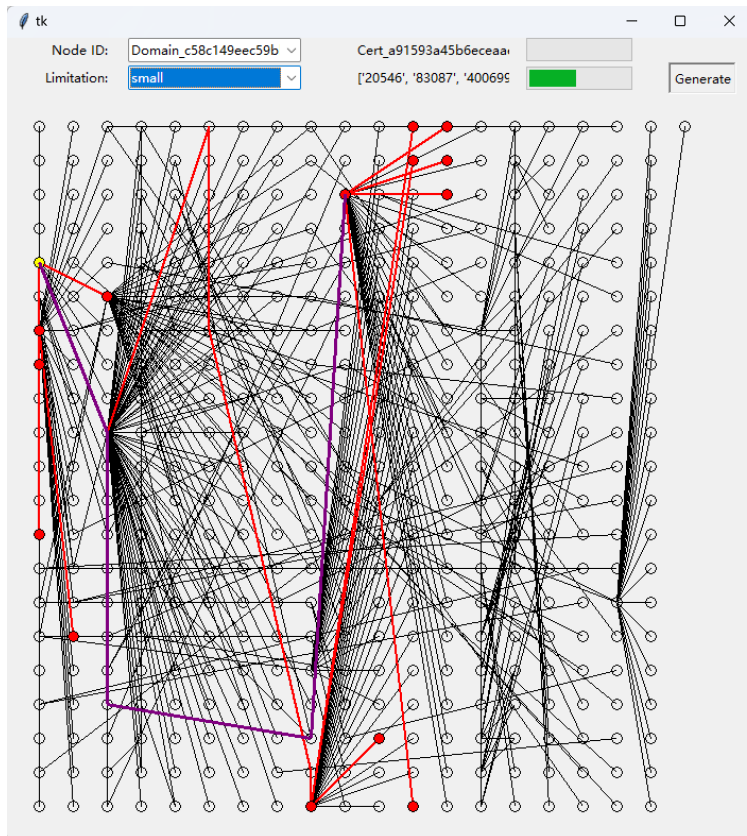
进度条代表当前还剩余多少节点或边，完成后点击其中一个蓝色节点



该节点即变黄，顶部将显示选中了哪个节点，关键路径被展示，可以再选择其他的红色节点



两个节点之间的关键路径就会用紫色展示，节点栏展示目标节点，边栏将展示路径信息。



再次点击黄色节点将会清除关键节点赋色。